(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月4 日 (04.08.2005)

PCT

(10) 国際公開番号
WO 2005/071878 A1

(51) 国際特許分類[7]: H04L 9/08, 9/32, G07C 13/00, G06F 17/60

(21) 国際出願番号: PCT/JP2005/000532

(22) 国際出願日: 2005 年1 月18 日 (18.01.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-016894 2004 年1 月26 日 (26.01.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目7－1 Tokyo (JP).

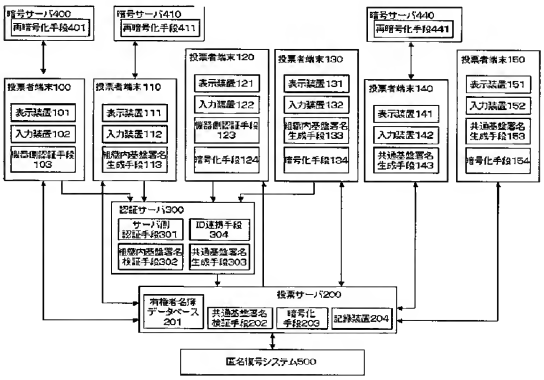
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 森 健吾 (MORI, Kengo) [JP/JP]; 〒1088001 東京都港区芝五丁目7－1 日本電気株式会社内 Tokyo (JP). 佐古 和恵 (SAKO, Kazue) [JP/JP]; 〒1088001 東京都港区芝五丁目7－1 日本電気株式会社内 Tokyo (JP).

[続葉有]

(54) Title: ANONYMOUS ELECTRONIC VOTING SYSTEM AND ANONYMOUS ELECTRONIC VOTING METHOD

(54) 発明の名称: 匿名電子投票システム及び匿名電子投票方法



400 ENCRYPTION SERVER
401 RE-ENCRYPTION MEANS
410 ENCRYPTION SERVER
411 RE-ENCRYPTION MEANS
440 ENCRYPTION SERVER
441 RE-ENCRYPTION MEANS
100 VOTER TERMINAL
101 DISPLAY DEVICE
102 INPUT DEVICE
103 DEVICE SIDE AUTHENTICATION MEANS
110 VOTER TERMINAL
111 DISPLAY DEVICE
112 INPUT DEVICE
113 IN-ORGANIZATION SUBSTRATE SIGNATURE CREATION MEANS
120 VOTER TERMINAL
121 DISPLAY DEVICE
122 INPUT DEVICE
123 DEVICE SIDE AUTHENTICATION MEANS
124 ENCRYPTION MEANS
130 VOTER TERMINAL
131 DISPLAY DEVICE
132 INPUT DEVICE
133 IN-ORGANIZATION SUBSTRATE SIGNATURE CREATION MEANS
134 ENCRYPTION MEANS
140 VOTER TERMINAL
141 DISPLAY DEVICE
142 INPUT DEVICE
143 COMMON SUBSTRATE SIGNATURE CREATION MEANS
150 VOTER TERMINAL
151 DISPLAY DEVICE
152 INPUT DEVICE
153 COMMON SUBSTRATE SIGNATURE CREATION MEANS
154 ENCRYPTION MEANS
300 AUTHENTICATION SERVER
301 SERVER SIDE AUTHENTICATION MEANS
304 ID LINKAGE MEANS
302 IN-ORGANIZATION SUBSTRATE SIGNATURE VERIFICATION MEANS
303 COMMON SUBSTRATE SIGNATURE CREATION MEANS
200 VOTING SERVER
201 VOTER LIST DATABASE
202 COMMON SUBSTRATE SIGNATURE VERIFICATION MEANS
203 ENCRYPTION MEANS
204 RECORDING DEVICE
500 ANONYMOUS DECRYPTION SYSTEM

(57) Abstract: An encrypted candidate name corresponding to a candidate selected from a combination list of a candidate name transmitted from a voting server (200) by voter terminals (100, 110, 140) and an encrypted candidate name, is transmitted to an encryption server (400) via a network. The encrypted candidate name is re-encrypted into encrypted voting data by the encryption server (400) and the data is returned to the voter terminals (100, 110, 140). Among them, a valid encrypted voting data list is created so that voting is performed in the voting server (200) via the network and an anonymous decoding system (500) decrypts the encrypted voting data.

[続葉有]

WO 2005/071878 A1

(74) 代理人: 稲垣 清, 外(INAGAKI, Kiyoshi et al.); 〒1010042 東京都千代田区神田東松下町３７ 林道ビル５階 扶桑特許事務所内 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

投票者端末（１００，１１０，１４０）により投票サーバ（２００）から送信された候補者名と暗号化候補者名との組み合わせリストの中から選択した候補者に対応する暗号化候補者名をネットワーク経由で暗号サーバ（４００）へ送信し、暗号化サーバ（４００）により該暗号化候補者名を再度暗号化した暗号化投票データを返信された投票者端末（１００，１１０，１４０）は、このうち有効な暗号化投票データリストを作成してネットワーク経由で投票サーバ（２００）に投票を行い、匿名復号システム（５００）により暗号化投票データの復号を行う。

明 細 書

匿名電子投票システム及び匿名電子投票方法

技術分野

[0001] 本発明は、匿名電子投票システム及び方法に関し、更に詳しくは、多様なクライアント環境から利用可能な匿名電子投票システム及び匿名電子投票方法に関する。

背景技術

[0002] 匿名電子投票システムは、例えばネットワークなどを介して無記名の秘密投票を電子的に実現するシステムであり、従来の匿名電子投票システムの一例が、特許文献1や非特許文献1に記載されている。なお、以下の説明において、投票には、予め定められている候補者から選挙を行うための投票のみならず、自由記述を許すアンケートなども含まれるものとする。また、候補者や候補者名は、単に選挙における候補者や候補者名を指すものではなく、ある集合から投票者の意思によってある要素あるいは項目を選択する場合のその要素(項目)や要素(項目)名をも含むものである。

[0003] 図28に示すように、従来の匿名電子投票システムは、窓口センタ901と複数の復号シャッフルセンタ902とからなる匿名復号システム900と、各投票者がアクセスすることとなる投票管理センタ(投票サーバ)910と、から構成されている。匿名復号システム900は、投票の秘密を守るために設けられており、投票者と暗号化投票データとの対応を秘匿して復号結果を出力するために用いられている。

[0004] 上記構成を有する従来の匿名電子投票システムは、次のように動作する。

[0005] まず、窓口センタ901と復号シャッフルセンタ902は、投票用の暗号化鍵などのシステムの公開情報を生成して投票管理センタ910に送信し、投票管理センタ910は、各投票者にその公開情報を通知する。

[0006] 投票期間が始まると各投票者は、公開情報に基づいて自分の投票内容を暗号化して暗号投票文を作成し、その暗号投票文に対して投票者のデジタル署名を生成し、暗号投票文とデジタル署名とを投票管理センタ910に送信する。その際、各投票者は、典型的には、自己のクライアント端末において暗号投票文やデジタル署名を作成し、各種のネットワークを介して自己のクライアント端末から投票管理センタ910に

対して暗号投票文とデジタル署名とを投票管理センタ910に送信する。投票管理センタ910は、受信したデジタル署名を検証し、有権者名簿をもとに投票者の投票権を確認し、重複投票がないことを確認した後、受信した暗号投票文を受け付ける。

[0007] 投票期間が終わると、投票管理センタ910は、投票の受け付けを終了し、投票開始から終了までに受け付けた暗号投票文のリストを匿名復号システム900の窓口センタ901に送付する。窓口センタ901は、復号シャッフルセンタ902を介して暗号投票文のリストを復号し、リストの順序を入れ替えることで平文の投票文のリストを得、平文の投票文のリストを投票管理センタ910に返送する。

[0008] 投票管理センタ910は、窓口センタ901から受け取った平文の投票文のリストにより、投票結果の集計を行なう。

特許文献1:特開2002−237810号公報

特許文献2:特開2001−251289号公報

特許文献3:特開2002−344445号公報

非特許文献1:佐古 和恵、外6名、"シャッフリングによる大規模電子投票システムの実現"、情報処理学会第62回全国大会、2001年3月

発明の開示

発明が解決しようとする課題

[0009] 従来の匿名電子投票システムでは、投票者が使用するクライアント端末が携帯電話機のような記憶容量や処理能力の乏しい機器である場合には、投票の秘密が守られた投票が難しい、という問題点がある。その理由は、従来の匿名電子投票システムで投票者が行なう暗号化処理プログラムは、記憶容量や処理能力の乏しい機器には実装するのが難しく、一方、他の機器に投票内容を送って暗号化処理を行なうこととすると、暗号化処理を行なう機器には投票内容がわかってしまうからである。

[0010] また、従来の匿名電子投票システムでは、広く一般の人を有権者とするような投票(例えば公職選挙)において、有権者の認証が困難であり、非有権者の投票や重複投票を防止することが難しい、という問題点もある。その理由は、従来の匿名電子投票システムでは、有権者の認証に利用するデジタル署名において、すべての投票者が共通の公開鍵認証基盤に登録されていることを前提としているが、現在、一般にはそ

のような基盤が普及していないためである。

[0011] そこで本発明の第1の目的は、携帯電話機などの記憶容量や処理能力の小さい機器からも投票の秘密を守りつつ投票を行なえる電子投票システム及び匿名電子投票方法を提供することである。

[0012] 本発明の第2の目的は、すべての有権者が共通の公開鍵認証基盤に登録されているような条件が整備されていない場合であっても、有権者認証の行なえる匿名電子投票システム及び匿名電子投票方法を提供することである。

課題を解決するための手段

[0013] 本発明は、第1の視点において、候補者名と暗号化候補者名との組合わせをリストとして含むデータを受信して、選択された候補者の前記暗号化候補者名をネットワーク経由で送信する投票者端末と、

前記暗号化候補者名を受信し再度暗号化して暗号化投票データを作成し、該暗号化投票データを、前記暗号化候補者名を送信した当該投票者端末に前記ネットワーク経由で返信する少なくとも1つの暗号サーバと、

前記投票者端末から暗号化投票データを受信し、該受信した暗号化投票データの内で有効な暗号化投票データのリストを作成し、該作成したリストを前記ネットワーク経由で送信する投票サーバと、

前記投票サーバから受信した前記有効な暗号化投票データのリストを復号し、該リストの順序を入れ換えた平文の候補者名リストを前記ネットワーク経由で送信する復号サーバとを備え、

前記投票サーバは、前記復号サーバから前記平文の候補者名リストを受信し、該受信した候補者名リストに基づいて投票結果を集計することを特徴とする電子投票システムを提供する。

[0014] 本発明の第1の視点に係る匿名電子投票システムの好ましい態様では、投票サーバは復号サーバ(匿名復号システム)と接続され、投票サーバには暗号化手段を備え、暗号化手段をもたない投票者端末は暗号サーバと接続されており、共通基盤署名生成手段をもたない投票者端末は認証サーバと接続される。暗号サーバには再暗号化手段を備え、認証サーバにはID連携手段と共通基盤署名生成手段を備える

。

[0015] 上記構成において、投票サーバは暗号化手段をもたない投票者端末に対しては平文の候補者名と暗号化された候補者名の組を送信し、暗号化手段をもたない投票者端末は、投票者の選んだ候補者名に対応する、暗号化された候補者名を、暗号サーバを介して再度暗号化してから投票サーバに送信し、投票サーバは、受信したすべての暗号データを匿名復号システムにより復号する。これにより、本発明の第1の目的を達成することができる。

[0016] また、共通基盤署名生成手段をもたない投票者端末は、認証サーバと通信を行なって組織内での個人認証を行ない、認証サーバは組織内に閉じた投票者IDをID連携手段により共通基盤におけるIDに変換し、このIDと投票データの組に認証サーバの共通基盤デジタル署名を付与して投票サーバに送信する。このように、既存の認証基盤を利用して個人認証を行なったことを認証サーバのデジタル署名により証明することで、本発明の第2の目的を達成することができる。

[0017] 本発明は、第2の視点において、ネットワークに接続された投票者端末と、

公開情報から前記投票者端末毎に第1暗号化パラメータを生成する第1データ変換手段を有し、前記第1暗号パラメータを前記投票者端末に送信する第1の暗号サーバと、

前記公開情報から前記投票者端末毎に第2暗号化パラメータを生成する第2データ変換手段を有し、前記第2暗号化パラメータを前記投票者端末に送信する第2の暗号サーバと、

前記投票者端末から暗号化投票データを受信し、該受信した暗号化投票データの内で有効な暗号化投票データのリストを作成し、該作成したリストを前記ネットワーク経由で送信する投票サーバと、

前記投票サーバから受信した前記有効な暗号化投票データのリストを復号し、該リストの順序を入れ換えた平文の候補者名リストを生成し、前記ネットワーク経由で送信する復号サーバとを備え、

前記投票サーバは、前記復号サーバから前記平文の候補者名リストを受信し、該受信した候補者名リストに基づいて投票結果を集計し、

前記投票者端末は、投票内容を前記第1及び第2暗号化パラメータに基づいて暗号化して暗号化投票データを生成する暗号化手段を有し、該暗号化投票データを前記投票サーバに送信することを特徴とする匿名電子投票システムを提供する。

[0018] 上記本発明の第2の視点に係る匿名電子投票システムの好ましい態様では、投票サーバが、第1の視点の匿名電子投票システムにおける暗号化手段にかえて第1の変換手段を備え、第1の視点の匿名電子投票システムにおける暗号サーバの再暗号化手段にかえて第2の変換手段を備え、投票者端末が暗号化手段(暗号データ作成手段)を備える。

[0019] 上記好ましい態様の第2の視点に係る匿名電子投票システムでは、投票サーバは、第1の変換手段により投票内容の暗号化処理に必要な演算の一部を行なってその結果である暗号パラメータを投票者端末へ送信し、暗号サーバも同様に第2の変換手段により投票内容の暗号化処理に必要な演算の一部を行なってその結果である暗号パラメータを投票者端末へ送信し、投票者端末では投票内容とともに、投票サーバから受信した第1の変換結果と暗号サーバから受信した第2の変換結果とを暗号データ作成手段に入力して暗号化投票データを作成することで、本発明の第1の目的を達成することができる。

発明の効果

[0020] 本発明の匿名電子投票システムは、記憶容量や処理能力の小さい機器からも電子投票を行なえる、という効果を有する。その理由は、暗号化処理のすべて、もしくは、暗号化処理のうちで計算量の多い変換処理を、投票者端末で行なう必要がないからである。

[0021] また本発明の匿名電子投票システムは、記憶容量や処理能力の小さい機器を使って電子投票を行なっても、投票の秘密を守ることができる、という効果を有する。その理由は、暗号化投票データの復号は復号サーバによって行なわれるため、すべての暗号化投票データが復号されても、どの投票者の暗号化投票データがどの平文に対応するかがわからないことと、投票内容の平文は投票サーバと暗号サーバの両方の処理により暗号化され、投票サーバや暗号サーバは、単独では投票された暗号化投票データを復号できないからである。

[0022] さらに本発明の好ましい態様のの匿名電子投票システムは、すべての有権者が共通の公開鍵認証基盤に登録されているような条件が整備されていなくても、不正投票を防止しつつ投票を行なえる、という効果を有する。その理由は、組織内に限られた認証手段しかもたない有権者を認証サーバが認証し、その投票データに認証サーバのデジタル署名を付与することで、認証サーバによる投票者の認証が行なわれているデータであることを確認できるからである。

発明を実施するための最良の形態

[0023] 次に、本発明の好ましい実施の形態について、図面を参照して詳細に説明する。

[0024] 《第1の実施形態》

図1は、本発明の第1の実施形態の匿名電子投票システムの構成を示している。この匿名電子投票システムは、それぞれ構成要素や処理能力などが異なっている投票者端末100, 110, 120, 130, 140, 150と、投票センタ(投票サーバ)200と、認証サーバ300と、暗号サーバ400, 410, 440と、匿名復号システム500とから構成される。暗号サーバ400, 410, 440は、それぞれ、投票者端末100, 110, 140と接続している。後述する説明から明らかなように、投票者端末100, 110, 120, 130, 140, 150からの投票センタ200への接続形態は多様であり、あるものは投票センタ200に直接接続し、別のものは認証サーバ300を介して投票センタ200に接続し、また別のものは、直接接続と認証サーバ300を介した接続とを併用している。ここでは簡単のため図示を省略するが、投票者端末100, 110, 120, 130, 140, 150は、それぞれ、複数存在してもかまわない。また、投票者端末ひとつにつきひとつの暗号サーバが接続される構成としてもよいし、いくつかの投票者端末がひとつの暗号サーバと接続される構成としてもよい。また、暗号サーバと認証サーバとが同一のサーバ上で動作することも可能である。

[0025] まず、各投票者端末100, 110, 120, 130, 140, 150の構成について説明する。

[0026] 投票者端末100は、ディスプレイなどの表示装置101と、ボタンやキーボードなどの入力装置102と、機器側認証手段103とを備え、投票サーバ200、認証サーバ300、暗号サーバ400と通信回線などにより接続されている。

[0027] 投票者端末110は、ディスプレイなどの表示装置111と、ボタンやキーボードなどの

入力装置112と、組織内基盤署名生成手段113とを備え、投票サーバ200、認証サーバ300、暗号サーバ410と通信回線などにより接続されている。

[0028] 投票者端末120は、ディスプレイなどの表示装置121と、ボタンやキーボードなどの入力装置122と、機器側認証手段123と、暗号化手段124とを備え、投票サーバ200、認証サーバ300と通信回線などにより接続されている。

[0029] 投票者端末130は、ディスプレイなどの表示装置131と、ボタンやキーボードなどの入力装置132と、組織内基盤署名生成手段133と、暗号化手段134とを備え、投票サーバ200、認証サーバ300と通信回線などにより接続されている。

[0030] 投票者端末140は、ディスプレイなどの表示装置141と、ボタンやキーボードなどの入力装置142と、共通基盤署名生成手段143とを備え、投票サーバ200、暗号サーバ440と通信回線などにより接続されている。

[0031] 投票者端末150は、ディスプレイなどの表示装置151と、ボタンやキーボードなどの入力装置152と、共通基盤署名生成手段153と、暗号化手段154とを備え、投票サーバ200と通信回線などにより接続されている。

[0032] 投票サーバ200は、有権者名簿データベース201と、共通基盤署名検証手段202と、暗号化手段203と、ハードディスクドライブなどの記録装置204とを備え、投票者端末100, 110, 120, 130, 140, 150及び認証サーバ300と通信回線などにより接続されている。

[0033] 認証サーバ300は、サーバ側認証手段301と、組織内基盤署名検証手段302と、共通基盤署名生成手段303と、ID連携手段304とを備えている。

[0034] 暗号サーバ400, 410, 440は、それぞれ再暗号化手段401, 411, 441を備えている。

[0035] 投票者端末100, 120の機器側認証手段103, 123は、認証サーバ300のサーバ側認証手段301と通信を行ない、投票者端末を操作している投票者の識別子がIDjであることの認証を受けるとともに、このサーバ側認証手段301と通信を行ない、投票者端末100, 120を操作している投票者jの識別子IDjを認証サーバ300に通知する。

[0036] 投票者端末120, 130, 140, 150と投票サーバ200とにそれぞれ設けられた暗号

化手段124，134，144，154，203は、暗号化公開鍵Yと平文投票データvを入力とし、Yによりvを暗号化した暗号化投票データE(v)を出力する。

[0037] 暗号サーバ400，410，440の再暗号化手段401，411，441は、いずれも、暗号化公開鍵Yと暗号化投票データE(v)を入力とし、YによりE(v)を再度暗号化した暗号化投票データE'(v)を出力する。

[0038] 投票者端末110，130の組織内署名生成手段113，133は、暗号化投票データE(vj)と投票者jの組織内識別子IIDjと署名用秘密鍵djとを入力とし、データ(E(vj)，IIDj)に対する投票者jの組織内向けデジタル署名Sejを出力する。

[0039] 認証サーバ300の組織内署名検証手段302は、暗号化投票データE(vj)と組織内識別子IIDjと組織内向けデジタル署名Sejと検証用公開鍵Pjとを入力とし、Sejがデータ(E(vj)，IIDj)に対して署名用秘密鍵djにより正しく計算されたものかどうかを判定する。

[0040] 投票者端末140，150の共通基盤署名生成手段143，153は、暗号化投票データE(vj)と投票者jの共通識別子CIDjと署名用秘密鍵djを入力とし、データ(E(vj)，CIDj)に対する投票者jの共通基盤デジタル署名Sejを出力する。

[0041] 認証サーバ300の共通基盤署名生成手段303は、暗号化投票データE(vj)と投票者jの共通識別子CIDjと、認証サーバの署名用秘密鍵dkを入力とし、データ(E(vj)，CIDj)に対する認証サーバの共通基盤デジタル署名Sekを出力する。

[0042] 投票センタ200の共通基盤署名検証手段202は、暗号化投票データE(vj)と共通識別子CIdjと共通基盤デジタル署名Sekを入力とし、Sekがデータ(E(vj)，CIDj)に対して署名用秘密鍵dkにより正しく計算されたものかどうかを判定する。

[0043] 認証サーバ300のID連携手段304には、組織内識別子IIDjと共通識別子CIDjとの対応関係が記録されており、組織内識別子IIDjが入力されると対応する共通識別子CIDjを出力する。

[0044] 匿名復号システム500は、外部から入力された初期設定情報に従って暗号化公開鍵Yを生成して出力し、外部から暗号化投票データE(vj)のリストが入力されると、E(vj)のリストを復号し、順番をランダムに並びかえた平文投票データvjのリストと、入力されたE(vj)のリストと出力したvjのリストとの間に1対1の対応関係があることの証明

データとを出力する。

[0045] 投票者端末110，130の組織内署名生成手段113，133と、投票者端末140，150の共通基盤署名生成手段143，153と、認証サーバ300の共通基盤署名生成手段303は、いずれもデジタル署名を作成するものであり、これに対し認証サーバ300の組織内署名検証手段302と投票サーバ200の共通基盤署名検証手段202とは、デジタル署名の検証を行うものである。ここでのデジタル署名には、例えばRSA暗号などの公開鍵暗号を用いるデジタル署名を用いることができる。RSA暗号を用いる場合、署名者jのデータVに対する署名Sjvは、Vと署名者jの署名用秘密鍵djを用いて、

Sjv＝V^dj mod n

により計算され、署名検証は、VとSjvと、djに対応する検証用公開鍵ejを用いて、

Sjv^ej＝V mod n

が成り立てば合格となる。なお、^はべき乗を表わす記号であり，V^djはVをdj回べき乗した結果（すなわちVdj）を表わす。

[0046] ここで、dj，ej，nは、二つの素数p，qに対して、

n＝p×q，

dj×ej＝1 mod （p−1）×（q−1）

と表わされる整数であり、あらかじめ各署名者jごとに相異なる（dj，ej）の組を作成し、djは各署名者jが秘密に保持し、（n，ej）の組は署名者jの識別子IDjと関連づけて公開しておくようにする。署名検証においては、公開されているIDjと（n，ej）との対応関係を検索して（n，ej）を取得して署名検証の処理を行なう。djは署名生成用秘密鍵、（n，ej）は署名検証用公開鍵とよばれる。

[0047] 組織内署名生成手段113，133及び組織内署名検証手段302においては、識別子IDjは例えば社員番号など、ある組織の内部でのみ公開・利用される組織内識別子であり、別々の組織に属する別の個人に割り振られた識別子が同じIDjになっている可能性もあり、また、有権者名簿に登録される有権者の識別子（有権者名など）との対応関係は公開されているとは限らない。IDjに対応する署名検証用公開鍵（n，ej）の組も同様に、組織の内部にのみ公開される場合もある。

[0048] 一方、共通基盤署名生成手段143，153，303及び共通基盤署名検証手段202においては、署名者の識別子IDjと(n，ej)とは広く一般に公開され、別の個人に同じ識別子が割り振られることのない、共通識別子であり、有権者名簿データベース201には共通識別子を含む情報が記録される。

[0049] 投票者端末100，120の機器側認証手段103，123と、認証サーバ300のサーバ側認証手段301は、個人認証を行うものである。ここでは、ID文字列とパスワードによる個人認証や、携帯電話の端末認証に基づいた個人認証などを用いることができる。

[0050] ID文字列とパスワードによる個人認証を行なう場合、認証サーバ300にはあらかじめ投票者の組織内識別子とパスワードの対応関係を記録しておく。機器側認証手段103，123は、入力装置102，122から入力された投票者の組織内識別子IIDjを認証サーバ300に送る。認証サーバ300は、サーバ側認証手段301により、受信したIIDjがあらかじめ記録された組織内識別子のリストに含まれることを確認し、乱数cを生成して投票者端末100，120へ返信する。機器側認証手段103，123は、入力装置102，122から入力されたパスワードpwと乱数cとをSHA1などのハッシュ関数に入力し、出力された値rを認証サーバ300に返信する。サーバ側認証手段301は、あらかじめ記録された組織内識別子とパスワードのリストをIIDjをキーとして検索し、IIDjに対応するpwを取得し、SHA1などのハッシュ関数にpwとcとを入力し、出力された値が投票者端末100，120から返信された値rと一致すれば、投票者端末100，120を操作している投票者をIIDjで示される投票者であると認める。

[0051] 本実施形態において、投票者端末120，130，150及び投票サーバ200に設けられる暗号化手段123，133，153，203と、暗号サーバ400，410，440に設けられる再暗号化手段401，411，441と、匿名復号システム500については、例えば特許文献1に示された技術を用いることができる。

[0052] 特許文献1に示された技術を用いる場合、匿名復号システム500は、投票センタ200からセキュリティパラメータ(pL，qL，t)とセッションIDが入力されると、(pL，qL，t)に従って公開情報(p，q，g)と秘密鍵Xを生成し、公開情報に公開鍵Yを加えた公開情報(p，q，g，Y)を出力して投票センタ200に返信する。ここで、p，qはエルガマル

暗号のパラメータであり、ある整数kにより

p＝k×q＋1という関係にある素数である。gは、法pにおける位数qの部分群を生成する生成元である。また、pL，qLは、素数p，qの長さであり、tは、順番入れ替え処理が正しいことを証明するためにデータの生成時および検証時に使用する繰り返し回数である。セッションIDは処理対象を識別するための識別子である。ここで、処理対象は、例えば県知事選挙、市議会議員選挙などである。公開鍵Yは復号鍵Xに対して、

Y＝g^X mod qの計算によって得られた値であり、復号鍵Xは無作為に選ばれたq未満の乱数である。

[0053] 暗号化手段123，133，153，203は、公開情報(p，q，g，Y)と平文投票データviを入力とし、暗号化投票データE(vi)を出力する。E(vi)は(Gi，Vi)という組で表され、

(Gi，Vi)＝(g^r mod p，vi×Y^r mod p)

の計算によって得られる。ここでrは、平文投票データviに対して無作為に選んだ乱数である。

[0054] なお本実施形態においては、このとき、正しくrを知って暗号化投票データを作成したことの証明を作成することができる。例えば、viの暗号化において乱数siを生成し、

αi＝g^si

mod p，

ci＝HASH(p，q，g，Y，Gi，Vi，αi)，

ti＝ci×ri＋si mod p

により、乱数証明データαi、tiを生成する。この証明は、

ci＝HASH(p，q，g，Gi，αi)を計算し、

g^ti×Gi^{−ci}＝αi mod p

が成り立つかどうかを確認することで検証できる。ここで、HASH(p，q，g，Y，Gi，Vi，αi)はSHA1などのハッシュ関数にp，q，g，Y，Gi，Vi，αiを入力して得られる値である。

[0055] 再暗号化手段401，411，441は、公開情報(p，q，g，Y)と暗号化投票データE(v

i)＝(Gi, Vi)を入力とし、暗号化投票データE'(vi)を出力する。E'(vi)は(G'i, V'i)という組で表され、

(G'i, V'i)＝(Gi×gˆs mod p, Vi×Yˆs mod p)

の計算によって得られる。ここで、sは暗号化投票データE(vi)に対して無作為に選んだ乱数である。なお、

(G'i, V'i)＝(Gi×gˆs mod p, Vi×Yˆs mod p)

＝(gˆ{r+s} mod p, vi×Yˆ{r+s} mod p)

の等式が成り立っており、E(vi)に対する復号処理と同じ処理をE'(vi)に施すことで平文投票データviを得ることができる。つまり、E(vi)とE'(vi)とは復号処理に関しては同様に扱える。

[0056] 投票センタ200がEi＝(Gi, Vi)のリストと、セッションIDとを匿名復号システム500に入力すると、匿名復号システム500は、セッションIDにより特定された公開情報(p, q, g, Y)および復号鍵Xにより(Gi, Vi)のリストを復号し、順番をランダムに並びかえた平文投票データviのリストと、(Gi, Vi)のリストとviのリストとの間に1対1の対応関係があることの証明データとを投票センタ200に返信する。

[0057] p, q, g, Xの生成、(Gi, Vi)のリストの復号と順番の並べかえ、(Gi, Vi)のリストとviとの間に1対1の対応関係があることの証明とその検証方法については、特許文献1に記載の方法を用いる。

[0058] ここでは、特許文献1の技術を用いる場合の、主に各構成要素の入出力について説明した。なお、暗号データのリストを、復号後に出力されるデータリストとの間に1対1の対応関係があることを、具体的な対応関係そのものの情報は一切漏らさずに証明する技術は、特開2001−251289号公報(特許文献2)、特開2002−344445号公報(特許文献3)などにも示されており、これらの技術を用いて暗号化手段123, 133, 153, 再暗号化手段401, 411, 441、匿名復号システム500を実現することも可能である。

[0059] 次に、本実施形態の匿名電子投票システムの全体の動作について説明する。

[0060] 図2には、この匿名電子投票システムでの初期設定の動作が記述されている。まず、投票サーバ200は、セキュリティパラメータ(pL, qL, t)とセッションIDとを匿名復号

システム500に送信する(ステップA1)。匿名復号システム500は、(pL, qL, t)にしたがって公開情報(p, q, g, Y)を作成し(ステップA2)、投票サーバ200へ返信する(ステップA3)。投票サーバ200は、(p, q, g, Y)を記録装置204に記録する(ステップA4)。以上により、初期設定が終了する。

[0061] 次に、図3ー図9を参照して、投票者端末100, 110, 120, 130, 140, 150を使った投票の動作を説明する。ここで、図3ー図8は、それぞれ、投票者端末100, 110, 120, 130, 140, 150での処理(及びそれらの投票者端末での処理に関連する投票サーバ、認証サーバ及び暗号サーバでの処理)を示している。また、図9は、投票受付け後から開票に相当する作業までの処理を説明している。

[0062] 投票期間が始まると、有権者である投票者は、投票者端末100, 110, 120, 130, 140, 150のいずれかにより投票サーバ200へアクセスする。このとき、投票者端末100, 110, 140からの投票では暗号投票情報要求を送信し(図3、図4、図7のステップA5−1)、投票者端末120, 130, 150からの投票では単なる投票情報要求を送信する(図5、図6、図8のステップA5−2)。投票サーバ200は、投票者端末100, 110, 140からの暗号投票情報要求を受信すると、その暗号化手段203により、すべての候補者名vjを公開情報(p, q, g, Y)で暗号化することによって(vj, E(vj))のリストを作成し(図3、図4、図7のステップA6)、公開情報(p, q, g, Y)と(vj, E(vj))のリストとを投票者端末100, 110, 140に返信する(図3、図4、図7のステップA7−1)。また、投票者端末120, 130, 150からの単なる投票情報要求を受信すると、投票サーバ200は、公開情報(p, q, g, Y)と平文の候補者名vjのリストとを投票者端末120, 130, 150に返信する(図5、図6、図8のステップA7−2)。

[0063] 以下、投票データの送信までの処理を、投票者端末100, 110, 120, 130, 140, 150ごとに別々に説明する。

[0064] 投票者端末100は、図3に示すように、(p, q, g, Y)と(vj, E(vj))のリストとを受信すると、その表示装置101においてvjのリストを投票者に対して表示し、投票者は入力装置102によりvjのリストから候補者名viを選択して入力する(ステップA100−1)。そして投票者端末100は、viに対応するE(vi)と公開情報(p, q, g, Y)とを暗号サーバ400に送信する(ステップA100−2)。次に、暗号サーバ400は、受信したE(vi)と

公開情報(p, q, g, Y)とを再暗号手段401に入力してE(vi)を再度暗号化したE'(vi)を計算し(ステップA100−3)、E'(vi)を投票者端末100に返信する(ステップA100−4)。次に、投票者端末100は、入力装置102により投票者の組織内識別子IIDiを取得し、機器側認証手段103により認証サーバ300に対して投票者iの組織内識別子IIDiの認証を行ない(ステップA100−5)、E'(vi)を認証サーバ300に送信する(ステップA100−6)。

[0065] 認証サーバ300は、サーバ側認証手段301により確認した投票者の組織内識別子IIDiをID連携手段304に入力し、対応する共通識別子CIDiを得る(ステップA100−7)。次に、認証サーバ300では、共通基盤署名生成手段303に(E'(vi), CIDi)の組と認証サーバ300の署名用秘密鍵dkとが入力されて、(E'(vi), CIDi)に対する認証サーバ300の共通基盤署名Sekが生成される(ステップA100−8)。そして、認証サーバ300は、(Ei, CIDi)=(E'(vi), CIDi)とSekとを投票サーバ200に送信する(ステップA100−9)。

[0066] 投票者端末110は、図4に示すように、(p, q, g, Y)と(vj, E(vj))のリストとを受信すると、その表示装置111においてvjのリストを投票者に対して表示し、投票者は入力装置112によりvjのリストから候補者名viを選択して入力する(図4のステップA110−1)。そして、投票者端末110は、viに対応するE(vi)と公開情報(p, q, g, Y)とを暗号サーバ410に送信する(図4のステップA110−2)。暗号サーバ410は、受信したE(vi)と公開情報(p, q, g, Y)とを再暗号手段411に入力してE(vi)を再度暗号化したE'(vi)を計算し(ステップA110−3)、E'(vi)を投票者端末110に返信する(ステップA110−4)。次に、投票者端末110は、組織内署名生成手段113に投票者iの組織内識別子IIDiと署名用秘密鍵diとE'(vi)とを入力し、(E'(vi), IIDi)に対する組織内向けデジタル署名Seiを計算し(ステップA110−5)、(E'(vi), IIDi)とSeiとを認証サーバ300に送信する(ステップA110−6)。

[0067] 認証サーバ300は、その組織内署名検証手段302により、Seiが(E'(vi), IIDi)に対して署名用秘密鍵diにより正しく計算されたものかどうかを検証し(ステップA110−7)、合格であれば、ID連携手段304によってIIDiに対応する共通識別子CIDiを取得する(ステップA110−8)。次に、認証サーバ300は、共通基盤署名生成手段303

にE'(vi)とCIDiと認証サーバ300の署名用秘密鍵dkとを入力して、(E'(vi), CIDi)に対する認証サーバ300の共通基盤デジタル署名Sekを出力し(ステップA110−9)、(Ei, CIDi)=(E'(vi), CIDi)とSekとを投票サーバ200に送信する(ステップA110−10)。

[0068] 投票者端末120は、図5に示すように、(p, q, g, Y)とvjのリストとを受信すると、その表示装置121においてvjのリストを投票者に対して表示し、投票者は入力装置122によりvjのリストから候補者名viを選択して入力する(ステップA120−1)。そして投票者端末120は、viと公開情報(p, q, g, Y)とを暗号化手段124に入力し、viをYにより暗号化したE(vi)を得る(ステップA120−2)。次に、投票者端末120は、機器側認証手段123により認証サーバ300に対して投票者iの組織内識別子IIDiの認証を行ない(ステップA120−3)、E(vi)を認証サーバ300に送信する(ステップA120−4)。

[0069] 認証サーバ300は、サーバ側認証手段301により確認した投票者の組織内識別子IIDiをID連携手段304に入力し、対応する共通識別子CIDiを得る(ステップA120−5)。次に、認証サーバ300は、共通基盤署名生成手段303に(E(vi), CIDi)の組と認証サーバ300の署名用秘密鍵dkを入力して、(E(vi), CIDi)に対する共通基盤署名Sekを生成し(ステップA120−6)、(Ei, CIDi)=(E(vi), CIDi)とSekとを投票サーバ200に送信する(ステップA120−7)。

[0070] 投票者端末130は、図6に示すように、(p, q, g, Y)とvjのリストとを受信すると、その表示装置131においてvjのリストを投票者に対して表示し、投票者は入力装置132によりvjのリストから候補者名viを選択して入力する(ステップA130−1)。そして投票者端末130は、viと公開情報(p, q, g, Y)とを暗号化手段134に入力し、viをYにより暗号化したE(vi)を得る(ステップA130−2)。次に投票者端末130は、組織内署名生成手段133に投票者iの組織内識別子IIDiと署名用秘密鍵diとE(vi)とを入力し、(E(vi), IIDi)に対する組織内向けデジタル署名Seiを計算し(ステップA130−3)、(E(vi), IIDi)とSeiとを認証サーバ300に送信する(ステップA130−4)。

[0071] 認証サーバ300は、組織内署名検証手段302により、Seiが(E(vi), IIDi)に対して署名用秘密鍵diにより正しく計算されたものかどうか検証し(ステップA130−5)、

合格であれば、ID連携手段304によりIIDiに対応する共通識別子CIDiを取得する(ステップA130—6)。次に認証サーバ300は、共通基盤署名生成手段303にE(vi)とCIDiと認証サーバ300の署名用秘密鍵dkとを入力して、(E(vi), CIDi)に対する認証サーバ300の共通基盤デジタル署名Sekを出力し(ステップA130—7)、(Ei, CIDi)=(E(vi), CIDi)とSekとを投票サーバ200に送信する(ステップA130—8)。

[0072] 投票者端末140は、図7に示すように、(p, q, g, Y)と(vj, E(vj))のリストとを受信すると、その表示装置141においてvjのリストを投票者に対して表示し、投票者は入力装置142によりvjのリストから候補者名viを選択して入力する(ステップA140—1)。そして投票者端末140は、viに対応するE(vi)と公開情報(p, q, g, Y)とを暗号サーバ440に送信する(ステップA140—2)。次に暗号サーバ440は、受信したE(vi)と公開情報(p, q, g, Y)とを再暗号手段441に入力してE(vi)を再度暗号化したE'(vi)を計算し(ステップA140—3)、E'(vi)を投票者端末140に返信する(ステップA140—4)。次に投票者端末140は、共通基盤署名生成手段143に投票者iの共通基盤識別子CIDiと署名用秘密鍵diとE'(vi)とを入力し、(E'(vi), CIDi)に対する共通基盤デジタル署名Seiを計算し(ステップA140—5)、(Ei, CIDi)=(E'(vi), CIDi)とSeiとを投票サーバ200に送信する(ステップA140—6)。

[0073] 投票者端末150は、図8に示すように、(p, q, g, Y)とvjのリストとを受信すると、表示装置151においてvjのリストを投票者に対して表示し、投票者は入力装置152によりvjのリストから候補者名viを選択し入力する(ステップA150—1)。そして投票者端末150は、viと公開情報(p, q, g, Y)とを暗号化手段154に入力してviをYにより暗号化したE(vi)を得る(ステップA150—2)。次に投票者端末150は、共通基盤署名生成手段153に投票者iの共通基盤識別子CIDiと署名用秘密鍵diとE(vi)とを入力し、(E(vi), CIDi)に対する共通基盤デジタル署名Seiを計算し(ステップA150—3)、(Ei, CIDi)=(E(vi), CIDi)とSeiとを投票サーバ200に送信する(ステップA150—4)。

[0074] 以上が、投票データの送信までの処理である。つづいて、投票データの受付けと投票締切後の開票集計処理について、図9を用いて説明する。

[0075] 投票サーバ200は、認証サーバ300から(Ei, CIDi)とSekとを受信すると、共通基

盤署名検証手段202によりSekが(Ei, CIDi)に対する認証サーバ300の正しい署名であることを確認し(ステップA8−1)、有権者名簿データベース201を検索してCIDiが登録されていることとCIDiの投票をまだ受付けていないこととを確認し(ステップA9−1)、投票データ記録装置204に(Ei, CIDi)とSekとを記録するとともに、有権者名簿データベース201にCIDiが投票済みであることを記録する(ステップA10−1)。また、投票サーバ200は、投票者端末140, 150から(Ei, CIDi)とSeiとを受信すると、共通基盤署名検証手段202によりSeiが(Ei, CIDi)に対する投票者iの正しい署名であることを確認し(ステップA8−2)、有権者名簿データベース201を検索してCIDiが登録されていることとCIDiの投票をまだ受付けていないこととを確認し(ステップA9−2)、投票データ記録装置204に(Ei, CIDi)とSekとを記録するとともに、有権者名簿データベース201にCIDiが投票済みであることを記録する(ステップA10−2)。

[0076] 投票が締め切られた後、投票サーバ200は、投票データ記録装置204に記録したすべてのEiのリストと、ステップA2で匿名復号システム500へ送信したセッションIDとを匿名復号システム500へ送信する(ステップA11)。匿名復号システム500は、セッションIDで指定された公開情報(p, q, g, Y)と秘密鍵Xとに基づいてEiのリストを復号し、順番を無作為に並べかえた平文投票データvjのリストと、Eiのリストとvjのリストとの間に1対1の対応関係が存在することの証明データzと、を作成し(ステップA12)、投票サーバ200に対してvjのリストとzとを返信する(ステップA13)。投票サーバ200は、受信した平文投票データvjのリストにより投票の集計を行い、集計結果を発表する(ステップA14)。

[0077] 次に、本実施形態の効果について説明する。

[0078] 本実施形態では、投票サーバ200が投票者端末100, 110, 140に暗号化投票データを送り、投票者が選んだ暗号化投票データを暗号サーバ400, 410, 440によりさらに暗号化して投票サーバ200に送信するため、暗号手段を備えない投票者端末からでも、投票の秘密を守りつつ、投票を行なえる。また、投票者端末100, 120に機器側認証手段103, 123を備え、認証サーバ300にサーバ側認証手段301を備えることでデジタル署名に依らない認証を行ない、認証サーバ300の共通基盤デジ

タル署名を付与して投票サーバ200に暗号化投票データを送ることで、署名生成手段を備えない投票者端末からも投票を行なえる。また、投票者端末110，130に組織内基盤署名生成手段113，133を備え、認証サーバ300に組織内基盤署名検証手段302とID連携手段304を備えることで、組織内向けデジタル署名が付与された暗号化投票データを認証サーバ300で検証し、組織内識別子から共通基盤識別子への変換を行なったのち、認証サーバ300の共通基盤デジタル署名を付与して投票サーバ200へ送ることで、すべての投票者が共通の公開鍵認証基盤に登録されていなくとも、投票を行なえる。

[0079] なお、ここでは認証サーバ300はひとつだけとして説明したが、投票者によって異なる組織に所属している場合には、組織ごとに別の認証サーバを導入することで対応が可能である。

[0080] 《第2の実施形態》

次に、本発明の第2の実施形態について図面を参照して説明する。図10に示した第2の実施形態の匿名電子投票システムは、図1に示された第1の実施形態の匿名電子投票システムにおいて、投票者端末100，110，140内にそれぞれ暗号データ作成手段104，114，144を設けるとともに、投票サーバ200の暗号化手段203に代えて第1の変換手段206と暗号化証明検証手段207とを設け、暗号サーバ400，410，440における再暗号化手段401，411，441に代えてそれぞれ第2の変換手段405，415，445を設け、さらに、変換検証手段701を備える変換検証サーバ700を加えたものである。

[0081] ここで第1の変換手段206は、公開情報を入力とし、第1の変換データ(第1暗号パラメータ)と第1の変換証明データとを出力するものである。

[0082] 第2の変換手段405，415，445は、公開情報を入力とし、第2の変換データ(第2暗号パラメータ)と第2の変換証明データとを出力する。

[0083] 暗号データ作成手段104，114，144は、公開情報、第1の変換データ、第1の変換証明データ、第2の変換データ、第2の変換証明データ及び平文の投票内容viを入力として、暗号化投票データE(vi)を出力するとともに、E(vi)を正しく生成したことを証明する暗号化証明を出力する。

[0084] 暗号化証明検証手段207は、公開情報と暗号化投票データE(vi)と暗号化証明データとを入力とし、E(vi)が正しく生成されたものかどうかを検証する。

[0085] 第1の変換手段206、第2の変換手段405, 415, 445、暗号データ作成手段104, 114, 144及び暗号化証明検証手段207は、匿名復号システム500に対して特許文献1に示された技術を用いる場合、以下のように動作する。

[0086] 第1の変換手段206は、公開情報(p, q, g, Y)が入力されると、q未満の乱数rとdとを無作為に選び、第1の変換データ(Gr, Yr, r)として、

(Gr, Yr, r)=(g^r mod p, Y^r mod p, r)

を計算して出力し、第1の変換証明データ(Gd, d)として、

(Gd, d)=(g^d mod p, d)を計算して出力する。

[0087] 第2の変換手段405, 415, 445は、公開情報(p, q, g, Y)が入力されると、q未満の乱数sを選び、第2の変換データ(Gs, Ys, s)として、

(Gs, Ys, s)=(g^s mod p, Y^s mod p, s)

を計算して出力し、第2の変換証明データ(Gu, u)として、

(Gu, u)=(g^u mod p, u)

を計算して出力する。ここで、uは無作為に選んだq未満の乱数である。

[0088] 暗号データ作成手段は、第1の変換データ(Gr, Yr, r)、第1の変換証明データ(Gd, d)、第2の変換データ(Gs, Ys, s)、第2の変換証明データ(Gu, u)及び平文の投票内容viが入力されると、暗号化投票データE(vi)として、

E(vi)=(Gr×Gs mod p, vi×Yr×Ys mod p)

を計算する。さらに、

α=Gu×Gd mod p,

c=HASH(p, q, g, Y, Gi, Vi, α),

t=c×(r+s)+u+d mod q

を計算して暗号化証明データ(α, t)を計算し、暗号化投票データ(Gi, Vi)とともにこの暗号化証明データ(α, t)を出力する。

[0089] 暗号化証明データによる証明は、暗号化証明検証手段207により

c=HASH(p, q, g, Y, Gi, Vi, α)

を計算し、

$g^t \times Gi^{\{-c\}} = \alpha \mod p$

が成り立つかどうかを確認することで行う。

[0090] 変換検証手段701は変換データ(Gr, Yr, r)と変換証明データ(Gd, d)とについて、公開情報(p, q, g, Y)から正しく作成されたものかどうかを検証する。匿名復号システム500に対して特許文献1に示された技術を用いる場合、変換検証手段701は公開情報(p, q, g, Y)と変換データ(Gr, Yr, r)と変換証明データ(Gd, d)とを入力とし、

$Gr = G^r \mod p,$

$Yr = Y^r \mod p,$

$Gd = Y^d \mod p$

の等式がいずれも成り立てば合格と判定し、どれかひとつでも成り立たなければ不合格と判定する。

[0091] 次に、本実施形態の匿名電子投票システムの動作について説明する。図11ー図13は、それぞれ、投票者端末100, 110, 140での処理(及びそれらの投票者端末での処理に関連する投票サーバ、認証サーバ及び暗号サーバでの処理)を示しており、図14は、投票受付け後から開票に相当する作業までの処理を説明している。なお、本実施形態での初期設定の動作は第1の実施の形態と同じであり、また、投票者端末120, 130, 150の動作も第1の実施の形態におけるものと同じであるから、これらの動作については記載を省略する。

[0092] 以下、投票者端末100, 110, 140による投票サーバ200へのアクセスから投票データの送信までの処理を説明する。

[0093] 投票者端末100, 110, 140は、投票情報要求と変換データ要求とを投票サーバ200へ送信する(図11、図12、図13のステップB5)。投票サーバ200は、変換データ要求を受信すると、その第1の変換手段206に公開情報(p, q, g, Y)を入力し、第1の変換データ(Gr, Yr, r)と第1の変換証明データ(Gd, d)とを作成し(図11、図12、図13ステップB6)、投票者端末100, 110, 140にこれら(p, q, g, Y), (Gr, Yr, r), (Gd, d)を返信する(図11、図12、図13のステップB7)。投票者端末100, 110,

140は、投票サーバ200から(p, q, g, Y), (Gr, Yr, r), (Gd, d)を受信すると、それぞれ暗号サーバ400, 410, 440に、(p, q, g, Y)と変換データ要求とを送信する(図11、図12、図13のステップB100−1、B110−1、B140−1)。暗号サーバ400, 410, 440は、公開情報(p, q, g, Y)と変換データ要求とを受信すると、それぞれその第2の変換手段405, 415, 445に公開情報(p, q, g, Y)を入力して第2の変換データ(Gs, Ys, s)と第2の変換証明データ(Gu, u)とを生成し(図11、図12、図13のステップB100−2、B110−2、B140−2)、投票者端末100, 110, 140に(Gs, Ys, s)と(Gu, u)とを返信する(図11、図12、図13のステップB100−3, B110−3, B140−3)。

[0094] 以下、投票データの送信までの処理のうち第1の実施の形態と異なる部分を、投票者端末100, 110, 140ごとに別々に説明する。

[0095] 投票者端末100は、図11に示すように、第1の変換データ(Gr, Yr, r)、第1の変換証明データ(Gd, d)、第2の変換データ(Gs, Ys, s)及び第2の変換証明データ(Gu, u)を受信すると、その暗号データ作成手段104に対して、投票者iが入力した投票内容viと、(Gr, Yr, r), (Gd, d), (Gs, Ys, s)及び(Gu, u)とを入力し、暗号化投票データE(vi)と暗号化証明データ(α, t)とを計算する(ステップB100−4)。そしてIIDiの認証ののちE(vi)と(α, t)とを認証サーバ300に送信する(ステップB100−6)。認証サーバ300は、(E(vi), (α, t), CIDi)に対する認証サーバ300の共通基盤デジタル署名Sekを作成し(ステップB100−8)、(E(vi), (α, t), CIDi)とSekとを投票サーバ200に送信する(ステップB100−9)。

[0096] 投票者端末110は、図12に示すように、第1の変換データ(Gr, Yr, r)、第1の変換証明データ(Gd, d)、第2の変換データ(Gs, Ys, s)及び第2の変換証明データ(Gu, u)を受信すると、投票者iが入力した投票内容viと、(Gr, Yr, r), (Gd, d), (Gs, Ys, s)及び(Gu, u)とを暗号データ作成手段114に入力し、暗号化投票データE(vi)と暗号化証明データ(α, t)とを計算する(ステップB110−4)。そして、投票者端末110は、(E(vi), (α, t), IIDi)に対する組織内向けデジタル署名Seiを作成し(ステップB110−5)、(E(vi), (α, t), IIDi)とSeiとを認証サーバ300に送信する(ステップB110−6)。認証サーバ300は、Seiが(E(vi), (α, t), IIDi)に対するIIDiの

正しい署名であることを確認し(ステップB110−7)、そのID連携手段304によりIIDiに対応する共通識別子CIDiを取得し(ステップA110−8)、(E(vi), (α, t), CIDi)に対する認証サーバ300の共通基盤デジタル署名Sekを作成し(ステップB110−9)、(Ei=E(vi), (α, t), CIDi)とSekとを投票サーバ200に送信する(ステップB110−10)。

[0097] 投票者端末140は、図13に示すように、第1の変換データ(Gr, Yr, r)、第1の変換証明データ(Gd, d)、第2の変換データ(Gs, Ys, s)及び第2の変換証明データ(Gu, u)を受信すると、投票者iが入力した投票内容viと(Gr, Yr, r), (Gd, d), (Gs, Ys, s)及び(Gu, u)とを暗号データ作成手段144に入力し、暗号化投票データE(vi)と暗号化証明データ(α, t)とを計算する(ステップB140−4)。そして、(E(vi), (α, t), CIDi)に対する共通基盤デジタル署名Seiを作成し(ステップB140−5)、(Ei=E(vi), (α, t), CIDi)とSeiとを投票サーバ200に送信する(ステップB140−6)。

[0098] 以上が投票データの送信までの処理である。続けて、投票データの受付け以降の処理について、図14を用いて、第1の実施の形態と異なる部分を説明する。

[0099] 投票サーバ200は、認証サーバ300から(Ei, (α, t), CIDi)とSekとを受信すると、共通基盤署名検証手段202によりSekが(Ei, CIDi)に対する認証サーバ300の正しい署名であることを確認し(ステップB8−1)、暗号化証明検証手段207により、Eiが正しく作られたものであることを確認し(ステップB9−1)、有権者名簿データベース201を検索してCIDiが登録されていることとCIDiの投票をまだ受付けていないこととを確認し(ステップB10−1)、投票データ記録装置204に(Ei, (α, t), CIDi)とSekとを記録するとともに、有権者名簿データベース201にCIDiが投票済みであることを記録する(ステップB11−1)。また、投票サーバ200は、投票者端末140, 150から(Ei, (α, t), CIDi)とSeiとを受信すると、共通基盤署名検証手段202によりSeiが(Ei, (α, t), CIDi)に対する投票者iの正しい署名であることを確認し(ステップB8−2)、暗号化証明検証手段207により、Eiが正しく作られたものであることを確認し(ステップB9−2)、有権者名簿データベース201を検索してCIDiが登録されていることとCIDiの投票をまだ受付けていないこととを確認し(ステップB10−2)、投票データ

記録装置204に(Ei, CIDi)とSekとを記録するとともに、有権者名簿データベース201にCIDiが投票済みであることを記録する(ステップB11−2)。

[0100] なお、投票者端末100, 110, 140により投票を行なった投票者は、投票データの受け付けが終わった後、投票サーバから受信した公開情報(p, q, g, Y)と第1の変換データ(Gr, Yr, r)、第1の変換証明データ(Gd, d)とを変換検証サーバ700の変換証明手段701に入力し、第1の変換データ、第1の変換証明データが正しく公開情報(p, q, g, Y)から作成されたものかどうかを検証してもよい。また、暗号サーバ400, 410, 440から受信した第2の変換データ(Gs, Ys, s)、第2の変換証明データ(Gu, u)についても、同様に変換検証サーバ700の変換検証手段701により、公開情報(p, q, g, Y)から正しく作成されたものかどうかを検証してもよい。

[0101] 投票締切り後の処理については、第1の実施の形態の場合と同じであるので、ここでは説明を省略する。

[0102] 次に、本実施形態の効果について説明する。

[0103] 本実施形態では、投票者端末100, 110, 140にそれぞれ暗号データ作成手段104, 114, 144を備え、投票サーバ200に第1の変換手段206を備え、暗号サーバ400, 410, 440にそれぞれ第2の変換手段405, 415, 445を備えることで、投票者端末100, 110, 140では複雑な演算を行なうことなく、暗号化投票データの作成が行なえる。また、暗号化投票データは第1の変換データと第2の変換データの両方をもとに計算されるため、投票サーバ200や暗号サーバ400, 410, 440は、単独では、投票者の暗号化投票データから平文の投票内容を知ることはできない。また、暗号データ作成手段104, 114, 144により生成される暗号化証明データは、投票者端末120, 130, 150の暗号化手段124, 134, 154が生成する暗号化証明データと同じ処理で検証が可能である。また、投票者端末100, 110, 140に暗号データ作成手段104, 114, 144を備えるため、投票内容となる候補者名などあらかじめ決められているような投票に限らず、投票者が自由に投票内容を決める自由記述による投票(やアンケート)などにも本実施形態は適用可能である。

[0104] また、投票サーバ200が送信する第1の変換データ、第1の変換証明データ、および、暗号サーバ400, 410, 440が送信する第2の変換データ、第2の変換証明デー

タは、変換検証手段701を用いることで、公開情報(p, q, g, Y)から正しく作成されたものかどうかを確認できる。そのため、投票サーバ200や暗号サーバ400, 410, 440が不正な変換データ、変換証明データを投票者端末に送信して投票を妨害しようとした場合、その不正が発覚する。これにより、投票サーバ200、暗号サーバ400, 410, 440での不正行為を抑止することができる。

[0105] 《第3の実施形態》

次に、本発明の第3の発明形態について図面を参照して説明する。図15に示した第3の実施形態の匿名電子投票システムは、図1に示された第1の実施形態の匿名電子投票システムにおいて、さらに暗号証明検証サーバ600を設けるとともに、投票サーバ200の暗号化手段203に代えて証明付き暗号化手段205を設け、暗号サーバ400, 410, 440の再暗号化手段401, 411, 441に代えてそれぞれ証明付き再暗号化手段402, 412, 442を設け、暗号証明検証サーバ600には暗号化証明検証手段601と再暗号化証明検証手段602とを設けたものである。

[0106] 証明付き暗号化手段205は、暗号化公開鍵Yを含む公開情報と平文データvとを入力とし、Yによりvを暗号化したE(v)と、E(v)がYによりvを正しく暗号化したことを示す証明データwとを出力する。証明付き再暗号化手段402, 412, 442は、暗号化公開鍵Yを含む公開情報と暗号データE(v)とを入力とし、YによりE(v)を再度暗号化したE'(v)と、E'(v)がYによりE(v)を正しく再度暗号化したことを示す証明データw'とを出力する。

[0107] 暗号化証明検証手段601は、暗号化公開鍵Yを含む公開情報と平文データvと暗号データE(v)と証明データwとを入力とし、E(v)がYによりvを正しく暗号化したものかどうかを検証する。再暗号化証明検証手段602は、暗号化公開鍵Yを含む公開情報と暗号データE(v)とE(v)を再度暗号化したE'(v)と証明データw'とを入力とし、E'(v)がYによりE(v)を正しく暗号化したものかどうかを検証する。

[0108] 特許文献1に示された技術を用いる場合、証明付き暗号化手段205は、公開情報(p, q, g, Y)と平文投票データviを入力とし、暗号化投票データE(vi)と証明データwとを出力する。E(vi)は(Gi, Vi)という組で表され、

(Gi, Vi) = (g^r mod p, vi×Y^r mod p)

の計算によって得られる。ここで、rは平文投票データviに対して無作為に選んだ乱数である。そして、証明データwとしてrが出力される。

[0109] 証明付き再暗号化手段205は、公開情報(p, q, g, Y)と暗号化投票データE(vi)=(Gi, Vi)とを入力とし、暗号化投票データE'(vi)と証明データw'とを出力する。E'(vi)は(G'i, V'i)という組で表され、

(G'i, V'i)=(Gi^s mod p, Vi×Y^s mod p)

の計算によって得られる。ここで、sは平文投票データviに対して無作為に選んだ乱数である。そして、証明データw'としてsが出力される。

[0110] 暗号化証明検証手段601は、viと(p, q, g, Y)とE(vi)=(Gi, Vi)とwとを入力とし、

Gi=g^w mod p,

Vi=vi×Y^w mod p

の等式が両方とも成り立てば証明を合格と判定し、どちらか一方でも等式が成り立たなければ証明を不正と判定する。

[0111] 再暗号化証明検証手段602は、(Gi, Vi)と(p, q, g, Y)とE'(vi)=(G'i, V'i)とw'とを入力とし、

G'i=Gi^w' mod p,

V'i=Vi×Y^w' mod p

の等式が両方とも成り立てば証明を合格と判定とし、どちらか一方でも等式が成り立たなければ証明を不正と判定する。

[0112] 次に、本実施形態の匿名電子投票システムの動作について説明する。図16ー図18は、それぞれ、投票者端末100, 110, 140での処理(及びそれらの投票者端末での処理に関連する投票サーバ、認証サーバ及び暗号サーバでの処理)を示しており、図19は、投票受付け後から開票に相当する作業までの処理を説明している。なお、本実施形態での初期設定の動作は第1の実施の形態と同じであり、また、投票者端末120, 130, 150の動作も第1の実施の形態におけるものと同じであるから、これらの動作については記載を省略する。

[0113] 以下、投票者端末100, 110, 140による投票サーバ200へのアクセスから投票デ

ータの送信までの処理を説明する。

[0114] 投票者端末100, 110, 140は、投票サーバ200に対し、暗号投票情報要求を送信する。投票サーバ200は、暗号投票情報要求を受信すると、証明付き暗号化手段205により、すべての候補者名vjについて、vjを公開情報(p, q, g, Y)で暗号化してE(vj)を作成し、そのE(vj)がvjを(p, q, g, Y)により正しく暗号化したものであることの証明データwjを作成し(図17、図18、図19のステップC6)、公開情報(p, q, g, Y)と(vj, E(vj), wj)のリストとを投票者端末100, 110, 140に返信する(図16、図17、図18のステップC7)。

[0115] また、暗号サーバ400, 410, 440は、投票者端末からE(vi)と公開情報(p, q, g, Y)とを受信すると、それぞれ証明付き再暗号手段402, 412, 442にE(vi)と(p, q, g, Y)を入力し、E(vi)を再度暗号化したE'(vi)とE(vi)から(p, q, g, Y)により正しく暗号化したことの証明データw'iとを作成し(図16、図17、図18のステップC100—1, C110—1, C140—1)、投票者端末100, 110, 140にE'(vi)とw'iとを返信する(図16、図17、図18のステップC100—2, C110—2, C140—2)。

[0116] 以上が投票データの送信までの処理のうち、第1の実施形態と異なる部分である。

[0117] 次に、図19のフローチャートを参照し、投票受付け後の投票者の処理について説明する。

[0118] 投票者端末100, 110, 140により投票を行なった投票者は、投票データの受付けが終わった後、投票サーバ200から受信した公開情報(p, q, g, Y)と(vj, E(vj), wj)のリストと、暗号サーバから受信した(E'(vi), w'i)とE(vi)とを暗号証明検証サーバ600に送信する(ステップC15)。暗号証明検証サーバ600は、公開情報(p, q, g, Y)と(vj, E(vj), wj)のリストとを暗号化証明検証手段601に入力し、すべてのE(vj)がvjを(p, q, g, Y)により正しく暗号化されているかどうかを検証し(ステップC16)、さらに、(E'(vi), E(vi), w')を再暗号化検証手段602に入力し、E'(vi)がE(vi)を(p, q, g, Y)により正しく再度暗号化したものかどうか検証し(ステップC17)、検証結果を出力する(ステップC18)。

[0119] 次に、本実施形態の効果について説明する。

[0120] 本実施形態では、投票サーバ200に証明付き暗号化手段205を備え、投票者端

末には(vj, E(vj), wj)のリストが送信され、暗号化証明検証手段601によりE(vj)がvjを(p, q, g, Y)により正しく暗号化されたものかどうかを確認できるため、投票サーバ200がvjを暗号化したものと偽って(vj, E(v'j), w)を投票者端末に送信した場合、その不正が発覚する。これにより、投票サーバ200での不正行為を抑止することができる。

[0121] また、暗号サーバ400, 410, 440にそれぞれ証明付き再暗号手段402, 412, 442を備え、投票者端末にはE'(vi), E(vi), w'が送信され、暗号化証明検証手段602によりE'(vi)がE(vi)を(p, q, g, Y)により正しく暗号化したものかどうかを確認できるため、暗号サーバがE(vi)を再度暗号化したものと偽ってE'(v), E(vi), w'を投票者端末に返信した場合、その不正が発覚する。これにより、暗号サーバ400, 410, 440での不正行為を抑止することができる。

[0122] なおここでは、暗号化証明検証手段601を別のサーバ(暗号証明検証サーバ600)に備え、投票終了後に検証を行なう構成を示したが、投票者端末内にその構成要素として暗号化証明検証手段を設け、投票中に検証を行なえるようにする構成も可能である。また、暗号化検証手段を構成要素として暗号サーバ内に設け、投票サーバの暗号証明の検証のみを投票中に行ない、暗号サーバの証明データの検証のみを投票後に行なう構成をとることも可能である。また、投票者端末に暗号化証明検証手段601と再暗号化証明検証手段602とを備え、投票中にすべての検証を行なう構成にしてもよい。

[0123] 《第4の実施形態》

次に、本発明の第4の実施形態について図面を参照して説明する。第1の実施形態の匿名電子投票システムにおいて、1つの投票者端末が複数の暗号サーバを用いるようにすることによって、投票の秘密をさらに頑強(ロバスト)に守ることができるようになる。本実施形態は、1つの投票者端末に対応する暗号サーバの台数を増やしたものである。

[0124] 図20に示した第4の実施形態の匿名電子投票システムは、図1に示された第1の実施形態の匿名投票システムにおいて、kを2以上の整数として、投票者端末100がk台の暗号サーバ400−1ー400−kと接続し、同様に投票者端末110, 140がそれぞ

れ暗号サーバ410－1～410－k、暗号サーバ440－1～440－kと接続されるようにしたものである。各暗号サーバ400－1～400－k，410－1～410－k，440－1～440－kには、それぞれ、再暗号化手段401－1～401－k，411－1～411－k，441－1～441－kが備えられている。投票者端末100，110，120，130，140，150、投票サーバ200及び認証サーバ300の構成は、図1に示した第1の実施形態の場合と同じである。

[0125] 次に、本実施形態の匿名電子投票システムの動作について説明する。図21～図23は、それぞれ、投票者端末100，110，140での処理（及びそれらの投票者端末での処理に関連する投票サーバ、認証サーバ及び暗号サーバでの処理）を示している。なお、本実施形態での初期設定の動作は第1の実施の形態と同じであり、また、投票者端末120，130，150の動作も第1の実施の形態におけるものと同じであるから、これらの動作については記載を省略する。

[0126] 以下、投票者端末100，110，140による投票サーバ200へのアクセスから投票データの送信までの処理を説明する。

[0127] 投票者端末100，110，140は、投票サーバ200へ暗号投票情報要求を送信する（図21、図22、図23のステップA5－1）。投票サーバ200は、暗号投票情報要求を受信すると、その暗号化手段203により、すべての候補者名vjについて、vjを公開情報（p，q，g，Y）で暗号化してE（vj）を作成し（図21、図22、図23のステップA6）、公開情報（p，q，g，Y）と（vj，E（vj））のリストとを投票者端末100，110，140に返信する（図21、図22、図23のステップA7－1）。投票者端末100，110，140は、（p，q，g，Y）と（vj，E（vj））のリストとを受信すると、その表示装置101，111，141においてvjのリストを投票者に表示し、投票者は入力装置102，112，142によりvjのリストから候補者viを選択して入力する（図21、図22、図23のステップA100－1、A110－1、A140－1）。

[0128] そして、投票者端末100，110，140は、viに対応する暗号データE（vi）と公開情報（p，q，g，Y）とを1番目の暗号サーバ400－1，410－1，440－1に送信する（図21、図22、図23のステップD101－1，D111－1，D141－1）。暗号サーバ400－1，410－1，440－1は、受信した暗号データE（vi）と公開情報（p，q，g，Y）とを再暗号化

手段401－1，410－1，440－1に入力してE(vi)を再度暗号化したE'1(vi)を計算し(図21、図22、図23のステップD101－2，D111－2，D141－2)、E'1(vi)を投票者端末100，110，140に返信する(図21、図22、図23のステップD101－3，D111－3，D141－3)。次に、投票者端末100，110，140は、1番目の暗号サーバ400－1，410－1，440－1から得たE'1(vi)を2番目の暗号サーバ400－2，410－2，440－2に対して送信することにより、E'1(vi)をもう一回暗号化させてE'2(vi)を得る。以下、このような処理をk個の暗号サーバ400－1ー400－k，410－1ー410－k，440－1ー440－kのすべてについて繰り返し、暗号データE'k(vi)を得る(図21、図22、図23のステップD10k－3，D11k－3，D14k－3)。暗号データE'k(vi)はE(vi)をk回にわたって再暗号化したデータに該当する。投票者端末100，110，140は、E'k(vi)を認証サーバ300や投票サーバ200へ送る暗号データE'(vi)とする(図21、図22、図23のステップD100－6，D110－5，D140－5)。以降の処理は、第1の実施形態における処理と同じである。

[0129] 次に、本実施形態の効果について説明する。

[0130] 本実施形態では、投票者端末100，110，140に、それぞれ、暗号サーバ400－1ー400－k、暗号サーバ410－1ー410－k、暗号サーバ440－1ー440－kが接続され、投票者端末100，110，140は、投票サーバ200から受信した暗号データE(vi)を合計k回にわたって再暗号化して得られるE'(vi)を投票サーバ200に送る。そのため、投票サーバとk個の暗号サーバとがすべて結託しない限り、E'(vi)から平文の投票内容viが判明することはなく、投票の秘密をより強く求めることができる。

[0131] なお、ここでは、投票者端末100，110，140に接続される暗号サーバの個数をいずれもk個としたが、同数である必要はなく、それぞれ別の数であってもよい。また、第1の実施形態と同じく、いくつかの投票者端末がいくつかの暗号サーバを共用することも可能である。

[0132] また、図15に示された第3の実施形態の場合と同様に、各暗号サーバには証明付き再暗号化手段を備え、暗号化の証明データを作成するようにしてもよい。

[0133] 《第5の実施形態》

次に、本発明の第5の実施形態について図面を参照して説明する。第2の実施形

態の匿名電子投票システムにおいて、1つの投票者端末が複数の暗号サーバを用いるようにすることによって、投票の秘密をさらに頑強(ロバスト)に守ることができるようになる。本実施形態は、1つの投票者端末に対応する暗号サーバの台数を増やしたものである。

[0134] 図24に示した第5の実施形態の匿名電子投票システムは、図10に示された第2の実施形態の匿名投票システムにおいて、kを2以上の整数として、投票者端末100がk台の暗号サーバ400−1ー400−kと接続し、同様に投票者端末110, 140がそれぞれ暗号サーバ410−1ー410−k、暗号サーバ440−1ー440−kと接続されるようにしたものである。各暗号サーバ400−1ー400−k, 410−1ー410−k, 440−1ー440−kには、それぞれ、第2の変換手段405−1ー405−k, 415−1ー415−k, 445−1ー445−kが備えられている。mは1≦m≦kである整数として、m番目の暗号サーバ400−m, 410−m, 440−mの第2の変換手段405−m, 415−m, 445−mは、第2の変換データ(Gsm, Ysm, sm)と第2の変換証明データ(Gum, um)を作成する。ここで、

(Gsm, Ysm, sm)＝(gˆsm mod p, Yˆsm mod p, sm),

(Gum, um)＝(gˆum mod p, um)

である。

[0135] 投票者端末100, 110, 140の暗号データ作成手段104, 114, 144は、投票サーバからの第1の変換データ(Gr, Yr, r)＝(gˆr mod p, Yˆr mop p, r)及び第1の変換証明データ(Gd, d)＝(gˆr mod p, d)と、k個の暗号サーバからのk個の第2の変換データ(Gs1, Ys1, s1)ー(Gsk, Ysk, sk)及びk個の第2の変換証明データ(Gu1, u1)ー(Guk, uk)と、平文の投票内容viとが入力されると、下記式にしたがって、暗号化投票データE(vi)を計算する。

[0136] E(vi)＝(Gi, Vi)

＝(Gr×Gs1×Gs2×…×Gsk mod p, vi×Yr×Ys1×Ys2×…×Ysk mod p)

さらに、暗号データ作成手段104, 114, 144は、

a＝Gu×Gd1×Gd2×…×Gdk mod p,

c＝HASH(p, q, g, Y, Gi, Vi, a),

t＝c×(r＋s1＋s2＋…＋sk)＋u＋d1＋d2＋…＋dk mod q

を計算して、暗号化証明データ(a, t)を計算し、暗号化投票データ(Gi, Vi)とともに出力する。

[0137] この証明は、暗号化証明検証手段207により、

c＝HASH(p, q, g, Y, Gi, Vi, a)

を計算して、

g^t×Gi^{−c}＝a mod p

が成り立つかどうかを確認することで、検証できる。

[0138] なお、投票者端末120, 130, 150、投票サーバ200及び認証サーバ300の構成は、図10に示した第2の実施形態の場合と同じである。

[0139] 次に、本実施形態の匿名電子投票システムの動作について説明する。図25ー図27は、それぞれ、投票者端末100, 110, 140での処理(及びそれらの投票者端末での処理に関連する投票サーバ、認証サーバ及び暗号サーバでの処理)を示している。なお、本実施形態での初期設定の動作は第2の実施の形態と同じであり、また、投票者端末120, 130, 150の動作も第2の実施の形態におけるものと同じであるから、これらの動作については記載を省略する。

[0140] 以下、投票者端末100, 110, 140による投票サーバ200へのアクセスから投票データの送信までの処理を説明する。

[0141] 投票者端末100, 110, 140は、投票サーバ200への変換データ要求を送信する(図25、図26、図27のステップB5)。投票サーバ200は、変換データ要求を受信すると、第1の変換手段206に公開情報(p, q, g, Y)を入力し、第1の変換データ(Gr, Yr, r)と第1の変換証明データ(Gd, d)とを作成し(図25、図26、図27のステップB6)、投票者端末100, 110, 140に、(p, q, g, Y), (Gr, Yr, r), (Gd, d)を返信する(図25、図26、図27のステップB7)。投票者端末100, 110, 140は、投票サーバ200から(p, q, g, Y), (Gr, Yr, r), (Gd, d)を受信すると、それぞれ、暗号サーバ400−1, 410−1, 440−1に(p, q, g, Y)と変換データ要求とを送信する(図25、図26、図27のステップE101−1, E111−1, E141−1)。暗号サーバ400−1, 410−1

，440－1は、公開情報（p，q，g，Y）と変換データ要求とを受信すると、それぞれ、第2の変換手段405－1，415－1，445－1に（p，q，g，Y）を入力して、第2の変換データ（Gs1，Ys1，s1）と第2の変換証明データ（Gu1，u1）とを生成し（図25、図26、図27のステップE101－2，E111－2，E141－2）、投票者端末100，110，140に、（Gs1，Ys1，s1）と（Gu1，u1）とを返信する（図25、図26、図27のステップE101－3，E111－3，E141－3）。次に、投票者端末100，110，140は、2番目の暗号サーバ400－1，410－1，440－1に対して同じ処理を繰り返し、以下同様にして、k個の暗号サーバ400－1ー400－k，410－1ー410－k，440－1ー440－kのすべてについて繰り返し、k個の第2の変換データ（Gs1，Ys1，s1）ー（Gsk，Ysk，sk）とk個の第2の変換証明データ（Gu1，u1）ー（Guk，uk）とを得る（図25、図26、図27のステップE10k－3，E11k－3，E14k－3まで）。

[0142] 続いて投票者端末100，110，140は、投票者が入力したviと、第1の変換データ（Gr，Yr，r）、第1の変換証明データ（Gd，d）、k個の第2の変換データ（Gs1，Ys1，s1）ー（Gsk，Ysk，sk）及びk個の第2の変換証明データ（Gu1，u1）ー（Guk，uk）とを暗号データ作成手段104，114，144に入力し、暗号化投票データE（vi）と暗号化証明データ（a，t）とを計算する（図25、図26、図27のステップE100－4，E110－4，E140－4）。これ以降の処理は、第2の実施形態の場合と同様である。

[0143] 次に、本実施形態の効果について説明する。

[0144] 本実施形態では、投票者端末100，110，140に、それぞれ、暗号サーバ400－1ー400－k、暗号サーバ410－1ー410－k、暗号サーバ440－1ー440－kが接続され、投票者端末100，110，140は、投票サーバ200から受信した第1の変換データとk個の暗号サーバから受信したk個の第2の変換データにより暗号データE（vi）を作成し、この暗号データE（vi）を投票サーバ200に送る。そのため、投票サーバとk個の暗号サーバがすべて結託しない限り、E'（vi）から平文の投票内容viが判明することはなく、投票の秘密をより強く求めることができる。

[0145] なお、ここでは、投票者端末100，110，140に接続される暗号サーバの個数をいずれもk個としたが、同数である必要はなく、それぞれ別の数であってもよい。また、第2の実施形態と同じく、いくつかの投票者端末がいくつかの暗号サーバを共用する

ことも可能である。

[0146] なお、投票サーバ200に第1の変換手段を備えない構成とし、k個の暗号サーバから受信した第2の変換データ、第2の変換証明データのみを用いて暗号化投票データE(vi)及び暗号化証明データ(α, t)を作成することとしてもよい。この場合、投票者端末100, 110, 140を含めすべての投票者端末は投票サーバ200に単なる投票情報要求を送信し、投票サーバ200はすべての投票者端末に対して公開情報(p, q, g, Y)と候補者情報を送信する。投票者端末100, 110, 140の暗号データ作成手段104, 114, 144は、k個の第2の変換データ(Gs1, Ys1, s1)ー(Gsk, Ysk, sk)及びk個の第2の変換証明データ(Gd1, d1)ー(Gdk, dk)により、下記のように暗号化投票データE(vi)、暗号化証明データ(α, t)を計算する。

[0147] $E(vi) = (Gi, Vi)$

$= (Gs1 \times Gs2 \times \cdots \times Gsk \mod p, vi \times Ys1 \times Ys2 \times \cdots Ysk \mod p)$

,

$\alpha = Gd1 \times Gd2 \times \cdots Gdk \mod p,$

$c = HASH(p, q, g, Y, Gi, Vi, \alpha),$

$t = c \times (s1 + s2 + \cdots sk) + d1 + d2 \cdots dk \mod q$

[0148] なお、投票サーバは、第1の変換データ、第1の変換証明データをあらかじめ計算しておくことも可能であるし、同様に、公開情報(p, q, g, Y)をあらかじめ暗号サーバに配布しておき、第2の変換データ、第2の変換証明データを事前に計算しておくようにすることも可能である。

[0149] 以上、本発明の好ましい実施の形態について説明したが、上述した匿名電子投票システムを構成する投票者端末、投票サーバ、認証サーバ、暗号サーバ及び暗号証明検証サーバは、いずれも、それらの機能を実現するためのコンピュータプログラムを、サーバ用コンピュータやパーソナルコンピュータなどのコンピュータに読み込ませ、そのプログラムを実行させることによっても実現できる。こうしたコンピュータプログラムは、磁気テープやCD−ROMなどの記録媒体によって、あるいは、ネットワークを介してコンピュータに読み込まれる。言い換えれば、投票者端末、投票サーバ、認証サーバ、暗号サーバ及び暗号証明検証サーバにおけるそれぞれの構成要素は、いず

れも、ソフトウェアによってもハードウェアによっても実現できるものである。

[0150] 特に、投票者端末を実現するためのコンピュータとしては、データ処理能力とネットワーク接続機能とを有する携帯電話機や各種の携帯情報端末(PDA)などの、コンピュータとして見たときには比較的処理能力や記憶能力が小さいものを使用することができる。

産業上の利用可能性

[0151] 本発明は、ネットワークなどを介した匿名電子投票システムという用途に適用できる。また、投票内容として自由記述を許すことにより、ネットワークなどを介した匿名電子アンケートシステムという用途に適用できる。

図面の簡単な説明

[0152] [図1]本発明の第1の発明形態の匿名電子投票システムの構成を示すブロック図である。

[図2]第1の実施形態における初期設定の動作を示すフローチャートである。

[図3]第1の実施形態における投票者端末100の動作を示すフローチャートである。

[図4]第1の実施形態における投票者端末110の動作を示すフローチャートである。

[図5]第1の実施形態における投票者端末120の動作を示すフローチャートである。

[図6]第1の実施形態における投票者端末130の動作を示すフローチャートである。

[図7]第1の実施形態における投票者端末140の動作を示すフローチャートである。

[図8]第1の実施形態における投票者端末150の動作を示すフローチャートである。

[図9]第1の実施形態における投票サーバ200の動作を示すフローチャートである。

[図10]本発明の第2の実施形態の匿名電子投票システムの構成を示すブロック図である。

[図11]第2の実施形態における投票者端末100の動作を示すフローチャートである。

[図12]第2の実施形態における投票者端末110の動作を示すフローチャートである。

[図13]第2の実施形態における投票者端末140の動作を示すフローチャートである。

[図14]第2の実施形態における投票サーバ200の動作を示すフローチャートである。

[図15]本発明の第3の実施形態の匿名電子投票システムの構成を示すブロック図である。

[図16]第3の実施形態における投票者端末100の動作を示すフローチャートである。

[図17]第3の実施形態における投票者端末110の動作を示すフローチャートである。

[図18]第3の実施形態における投票者端末140の動作を示すフローチャートである。

[図19]第3の実施形態における暗号検証サーバ600の動作を示すフローチャートである。

[図20]本発明の第4の実施形態の構成を示すブロック図である。

[図21]第4の実施形態における投票者端末100の動作を示すフローチャートである。

[図22]第4の実施形態における投票者端末110の動作を示すフローチャートである。

[図23]第4の実施形態における投票者端末140の動作を示すフローチャートである。

[図24]本発明の第5の実施形態の構成を示すブロック図である。

[図25]第5の実施形態における投票者端末100の動作を示すフローチャートである。

[図26]第5の実施形態における投票者端末110の動作を示すフローチャートである。

[図27]第5の実施形態における投票者端末140の動作を示すフローチャートである。

[図28]従来の匿名電子投票システムの構成を示すブロック図である。

請求の範囲

[1] 候補者名と暗号化候補者名との組合わせをリストとして含むデータを受信して、選択された候補者の前記暗号化候補者名をネットワーク経由で送信する投票者端末(100、110, 140)と、

前記暗号化候補者名を受信し再度暗号化して暗号化投票データを作成し、該暗号化投票データを、前記暗号化候補者名を送信した当該投票者端末(100、110, 140)に前記ネットワーク経由で返信する少なくとも1つの暗号サーバ(400、410, 440)と、

前記投票者端末(100, 110, 140)から暗号化投票データを受信し、該受信した暗号化投票データの内で有効な暗号化投票データのリストを作成し、該作成したリストを前記ネットワーク経由で送信する投票サーバ(200)と、

前記投票サーバ(200)から受信した前記有効な暗号化投票データのリストを復号し、該リストの順序を入れ換えた平文の候補者名リストを前記ネットワーク経由で送信する復号サーバ(500)とを備え、

前記投票サーバ(200)は、前記復号サーバ(500)から前記平文の候補者名リストを受信し、該受信した候補者名リストに基づいて投票結果を集計することを特徴とする匿名電子投票システム。

[2] 選択した候補者の候補者名を暗号化して暗号化候補者名を生成する暗号化手段(124, 134, 154)を有する別の投票者端末(120, 130, 150)を更に備える、請求項1に記載の匿名電子投票システム。

[3] 投票者名簿に含まれる投票者又は投票者端末の識別情報をリストとして記憶する記憶装置を有し、前記投票者端末(100, 110, 120, 130)から前記暗号化投票データ及び識別情報を受信し、前記記憶装置に記憶された識別情報に基づいて前記暗号化投票データを認証する認証サーバ(300)を更に備え、前記投票サーバ(200)は、少なくとも該認証サーバ(300)により認証情報が付加された暗号化投票データを前記有効な暗号化投票データとして認める、請求項1又は2に記載の匿名電子投票システム。

[4] 認証サーバ(300)を更に備えており、

前記投票者端末(110, 130)は、前記暗号化投票データと、組織内識別情報と、秘密鍵とに基づいて、組織内デジタル署名を生成する組織内署名生成手段(113, 133)を有し、

前記認証サーバ(300)は、前記投票者端末(110, 130)から前記暗号化投票データと、組織内識別情報と、組織内デジタル署名とを受信し、公開鍵に基づいて前記組織内デジタル署名を認証し、

前記投票サーバ(200)は、少なくとも前記認証サーバ(300)により認証情報が付加された暗号化投票データを前記有効な暗号化投票データとして認める、請求項1又は2に記載の匿名電子投票システム。

[5] 前記少なくとも1つの暗号サーバが、前記暗号化候補者名を順次に多重に暗号化する1群の暗号サーバ(400−1ー400−k、410−1ー410−k、440−1ー440−k)を含み、前記投票サーバ(200)は、該1群の暗号サーバ(400−1ー400−k、410−1ー410−k、440−1ー440−k)で多重に暗号化された暗号化投票データを受信する、請求項1ー4の何れか一に記載の匿名電子投票システム。

[6] 前記リストに含まれる各組み合わせが、候補者名及び暗号化候補者名に加えて、候補者名を正当に暗号化した旨を示す証明データを含み、

前記暗号サーバ(400、410, 440)は、前記暗号化投票データに加えて、該暗号化投票データの正当性を示す証明データを作成して、前記投票者端末(100, 110, 140)に返信する、請求項1又は2に記載の匿名電子投票システム。

[7] ネットワークに接続された投票者端末(100, 110, 140)と、

公開情報から前記投票者端末(100, 110, 140)毎に第1暗号化パラメータを生成する第1データ変換手段(206)を有し、前記第1暗号パラメータを前記投票者端末(100, 110, 140)に送信する第1の暗号サーバ(200)と、

前記公開情報から前記投票者端末(100, 110, 140)毎に第2暗号化パラメータを生成する第2データ変換手段(405, 415, 445)を有し、前記第2暗号化パラメータを前記投票者端末(100, 110, 140)に送信する第2の暗号サーバ(400, 410, 440)と、

前記投票者端末(100, 110, 140)から暗号化投票データを受信し、該受信した

暗号化投票データの内で有効な暗号化投票データのリストを作成し、該作成したリストを前記ネットワーク経由で送信する投票サーバ(200)と、

前記投票サーバ(200)から受信した前記有効な暗号化投票データのリストを復号し、該リストの順序を入れ換えた平文の候補者名リストを生成し、前記ネットワーク経由で送信する復号サーバ(500)とを備え、

前記投票サーバ(200)は、前記復号サーバ(500)から前記平文の候補者名リストを受信し、該受信した候補者名リストに基づいて投票結果を集計し、

前記投票者端末(100, 110, 140)は、投票内容を前記第1及び第2暗号化パラメータに基づいて暗号化して暗号化投票データを生成する暗号化手段(104, 114, 144)を有し、該暗号化投票データを前記投票サーバ(200)に送信することを特徴とする匿名電子投票システム。

[8] 前記第1の暗号サーバ(200)と前記投票サーバ(200)とが同一のサーバ上で作動する、請求項7に記載の匿名電子投票システム。

[9] 前記投票者端末(100, 110, 140)は、前記暗号化投票データに加えて、暗号化証明データを作成して前記投票サーバ(200)に送信し、

前記投票サーバ(200)は、少なくとも前記暗号化証明データを検証して正当性を検証した後に、対応する暗号化投票データを前記有効な暗号化投票データとして認める、請求項7又は8に記載の匿名電子投票システム。

[10] 投票者名簿に含まれる投票者又は投票者端末の識別情報をリストとして記憶する記憶装置を有し、前記投票者端末(100)から前記暗号化投票データ及び識別情報を受信し、前記記憶装置に記憶された識別情報に基づいて前記暗号化投票データを認証する認証サーバ(300)を更に備え、前記投票サーバ(200)は、少なくとも前記認証サーバ(300)により認証情報が付加された暗号化投票データを前記有効な暗号化投票データとして認める、請求項7ー9の何れか一に記載の匿名電子投票システム。

[11] 認証サーバ(300)を更に備えており、

前記投票者端末(110)は、前記暗号化投票データと、組織内識別情報と、秘密鍵とに基づいて、組織内デジタル署名を生成する組織内署名生成手段(113)を有し、

前記認証サーバ(300)は、前記投票者端末(110)から前記暗号化投票データと、組織内識別情報と、組織内デジタル署名とを受信し、公開鍵に基づいて前記組織内デジタル署名を認証し、

前記投票サーバ(200)は、少なくとも前記認証サーバ(300)により認証情報が付加された暗号化投票データを前記有効な暗号化投票データとして認める、請求項7ー9の何れか一に記載の匿名電子投票システム。

[12] 投票サーバと投票者が投票を行うための投票者端末と暗号サーバと復号サーバとを用いる匿名電子投票方法であって、

前記投票サーバ(200)から、候補者名を暗号化して候補者名とその候補者名を暗号化した暗号化候補者名との組のリストを投票者端末(100, 110, 140)に送信する段階と、

前記投票者端末(100, 110, 140)から、投票者が選択した候補者名と組となった暗号化候補者名を前記暗号サーバ(400, 410, 440)に送信する段階と、

前記暗号サーバ(400, 410, 440)で、前記暗号化候補者名を再度暗号化して暗号化投票データを生成し、該生成した暗号化投票データを前記暗号化候補者名を送信した当該投票者端末(100, 110, 140)に送信する段階と、

前記投票者端末(100, 110, 140)から、前記暗号サーバ(400, 410, 440)から受信した暗号化投票データを前記投票サーバ(200)に送信する段階と、

前記投票サーバ(200)で、前記暗号化投票データを受付け、有効な暗号化投票データのリストを作成し送信する段階と、

前記復号サーバ(500)で、前記暗号化投票データのリストを復号して順序を入れ換えた平文の候補者名のリストを出力する段階と、

前記投票サーバ(200)で、前記平文の候補者名リストを受信し、該受信した候補者名リストに基づいて投票結果を集計する段階とを備えることを特徴とする匿名電子投票方法。

[13] 前記投票者端末(100)から前記暗号化投票データ及び識別情報を認証サーバ(300)で受信し、記憶装置に記憶された識別情報に基づいて前記暗号化投票データを認証し前記投票サーバ(100)に送信する段階と、前記投票サーバ(200)で、少な

くとも前記認証情報が付加された暗号化投票データを前記有効な暗号化投票データとして認める段階とを更に備える、請求項12に記載の匿名電子投票方法。

[14] 前記投票者端末(110)で、前記暗号化投票データと、組織内識別情報と、秘密鍵とに基づいて、組織内デジタル署名を生成する段階と、

認証サーバ(220)で、前記投票者端末(110)から前記暗号化投票データと、組織内識別情報と、組織内デジタル署名とを受信し、公開鍵に基づいて前記組織内デジタル署名を認証する段階と、

前記投票サーバ(200)で、少なくとも前記認証サーバ(300)により認証情報が付加された暗号化投票データを前記有効な暗号化投票データとして認める段階とを更に備える、請求項12に記載の匿名電子投票方法。

[15] 前記暗号化候補者名を再度暗号化する段階が、1群の暗号サーバ(400−1ー400−k、410−1ー410−k、440−1ー440−0k)で前記暗号化候補者名を順次に多重に暗号化して前記暗号化投票データを生成する段階である、請求項12に記載の匿名電子投票方法。

[16] 前記リストに含まれる各組合わせが、候補者名及び暗号化候補者名に加えて、候補者名を正当に暗号化した旨を示す証明データを含み、

前記暗号サーバ(400、410, 440)が、前記暗号化投票データと共に該暗号化投票データの正当性を示す証明データを作成して、前記投票者端末(100, 110, 140)に返信する、請求項12に記載の匿名電子投票方法。

[17] 第1の暗号サーバ(200)で、公開情報から前記投票者端末(100, 110, 140)毎に第1暗号化パラメータを生成し、該第1暗号パラメータを投票者端末(100, 110, 140)に送信する段階と、

第2の暗号サーバ(400, 410, 440)で、前記公開情報から前記投票者端末(100, 110, 140)毎に第2暗号化パラメータを生成し、該第2暗号化パラメータを前記投票者端末(100, 110, 140)に送信する段階と、

前記投票者端末(100, 110, 140)で、投票者の投票内容を前記第1及び第2暗号化パラメータに基づいて暗号化して暗号化投票データを生成し、該暗号化投票データを投票サーバ(200)に送信する段階と、

投票サーバ(200)で、受信した暗号化投票データの内で有効な暗号化投票データのリストを作成し、該作成したリストを前記ネットワーク経由で送信する段階と、

復号サーバ(500)で、前記投票サーバ(200)から受信した前記有効な暗号化投票データのリストを復号し、該リストの順序を入れ換えた平文の候補者名リストを作成して、前記ネットワーク経由で送信する段階と、

前記投票サーバ(200)で、前記平文の候補者名リストを受信し、該受信した候補者名リストに基づいて投票結果を集計する段階とを備えることを特徴とする匿名電子投票方法。

[18] 前記暗号化投票データを作成する段階が、前記暗号化投票データの正当性を証明する暗号化証明データを作成し、

前記投票サーバ(200)で、少なくとも前記暗号化証明データを検証して正当性を検証した後に、対応する暗号化投票データを前記有効な暗号化投票データとして認める段階を更に備える、請求項17に記載の匿名電子投票方法。

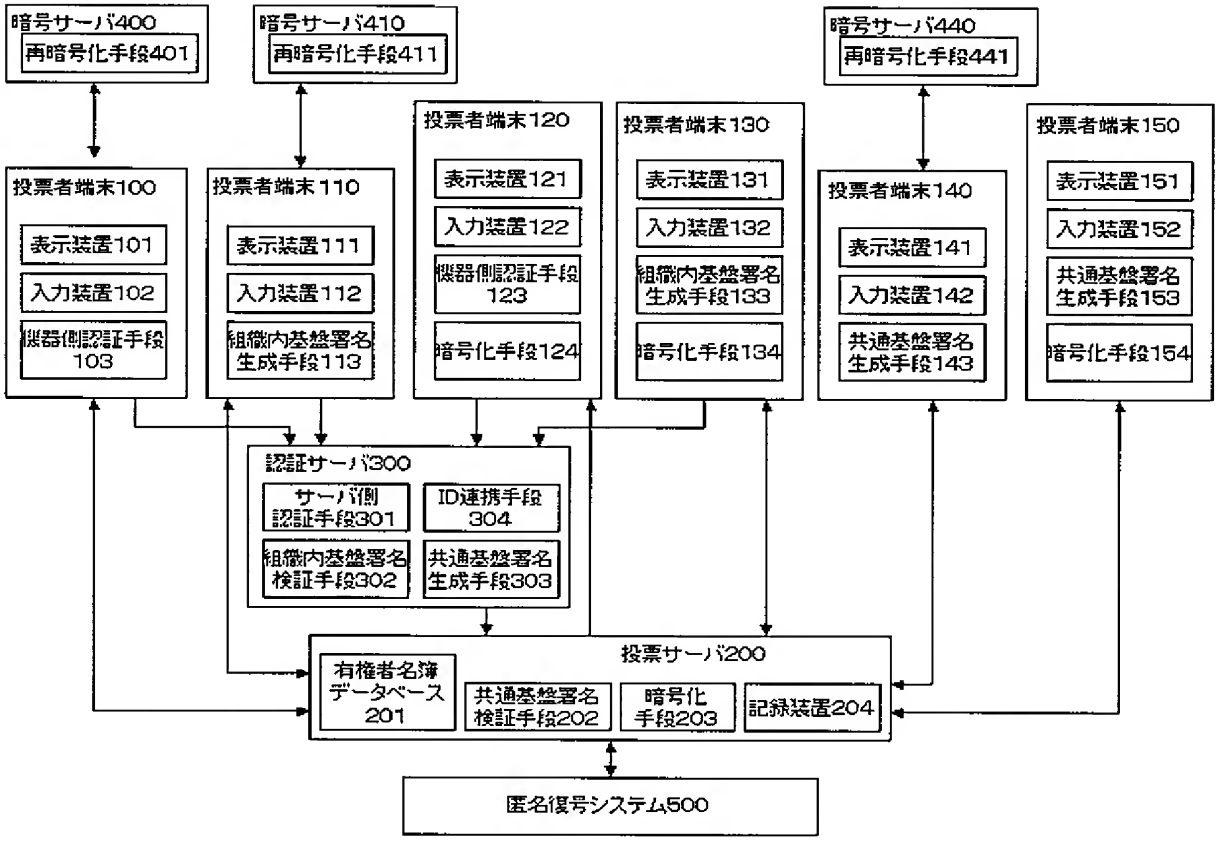
[19] 認証サーバ(300)で、前記投票者端末(100)から前記暗号化投票データ及び識別情報を受信し、記憶装置に記憶された識別情報に基づいて前記暗号化投票データを認証する段階と、前記投票サーバ(200)で、少なくとも前記認証情報が付加された暗号化投票データを前記有効な暗号化投票データとして認める段階とを更に備える、請求項17に記載の匿名電子投票方法。

[20] 前記投票者端末(110)で、前記暗号化投票データと、組織内識別情報と、秘密鍵とに基づいて、組織内デジタル署名を生成する段階と、

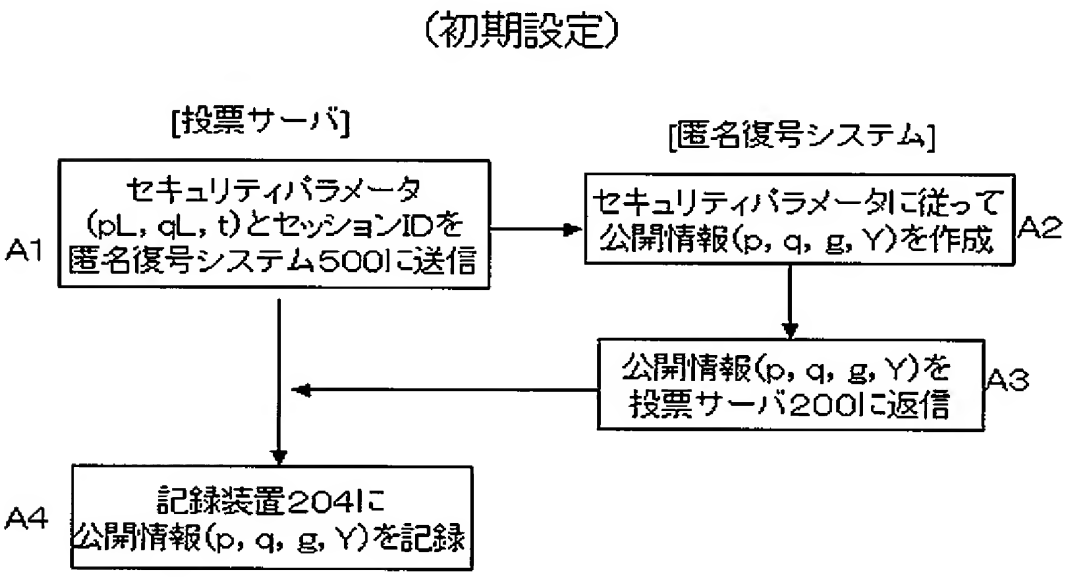
前記認証サーバ(300)で、前記投票者端末(110)から前記暗号化投票データと、組織内識別情報と、組織内デジタル署名とを受信し、公開鍵に基づいて前記組織内デジタル署名を認証する段階と、

前記投票サーバ(200)で、少なくとも前記認証情報が付加された暗号化投票データを前記有効な暗号化投票データとして認める段階とを更に備える、請求項17に記載の匿名電子投票方法。

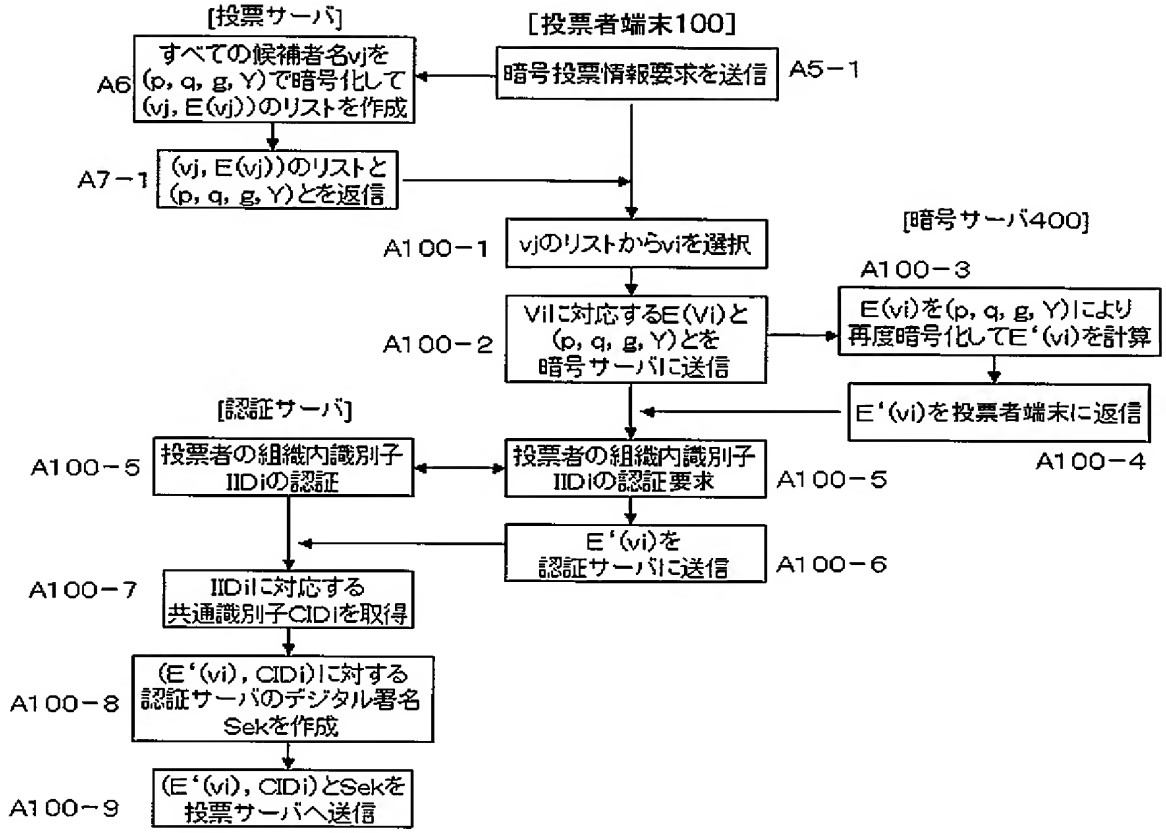
[図1]


暗号サーバ400
再暗号化手段401
暗号サーバ410
再暗号化手段411
暗号サーバ440
再暗号化手段441
投票者端末100
表示装置101
入力装置102
機器側認証手段103
投票者端末110
表示装置111
入力装置112
組織内基盤署名生成手段113
投票者端末120
表示装置121
入力装置122
機器側認証手段123
暗号化手段124
投票者端末130
表示装置131
入力装置132
組織内基盤署名生成手段133
暗号化手段134
投票者端末140
表示装置141
入力装置142
共通基盤署名生成手段143
投票者端末150
表示装置151
入力装置152
共通基盤署名生成手段153
暗号化手段154
認証サーバ300
サーバ側認証手段301
ID連携手段304
組織内基盤署名検証手段302
共通基盤署名生成手段303
投票サーバ200
有権者名簿データベース201
共通基盤署名検証手段202
暗号化手段203
記録装置204
匿名復号システム500

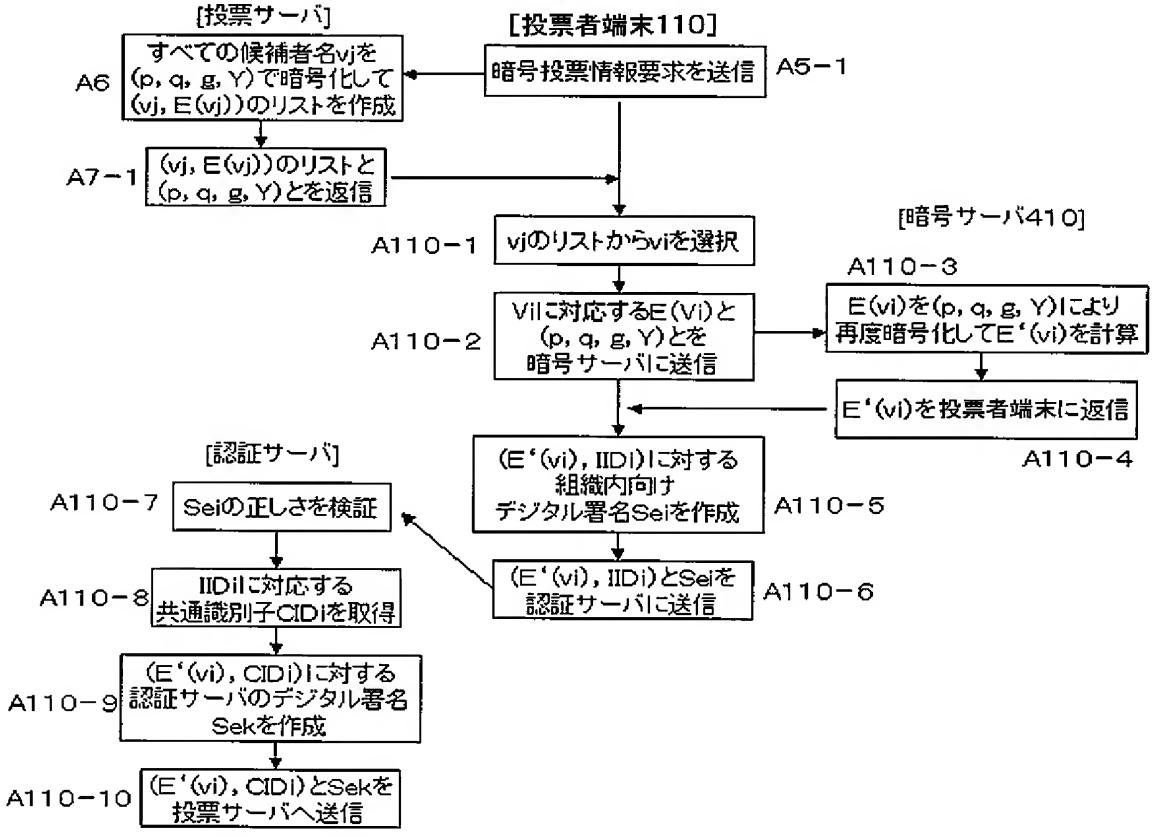
[図2]


(初期設定)
[投票サーバ]
[匿名復号システム]
A1
セキュリティパラメータ(pL, qL, t)とセッションIDを匿名復号システム500に送信
セキュリティパラメータに従って公開情報(p, q, g, Y)を作成
A2
公開情報(p, q, g, Y)を投票サーバ200に返信
A3
A4
記録装置204に公開情報(p, q, g, Y)を記録

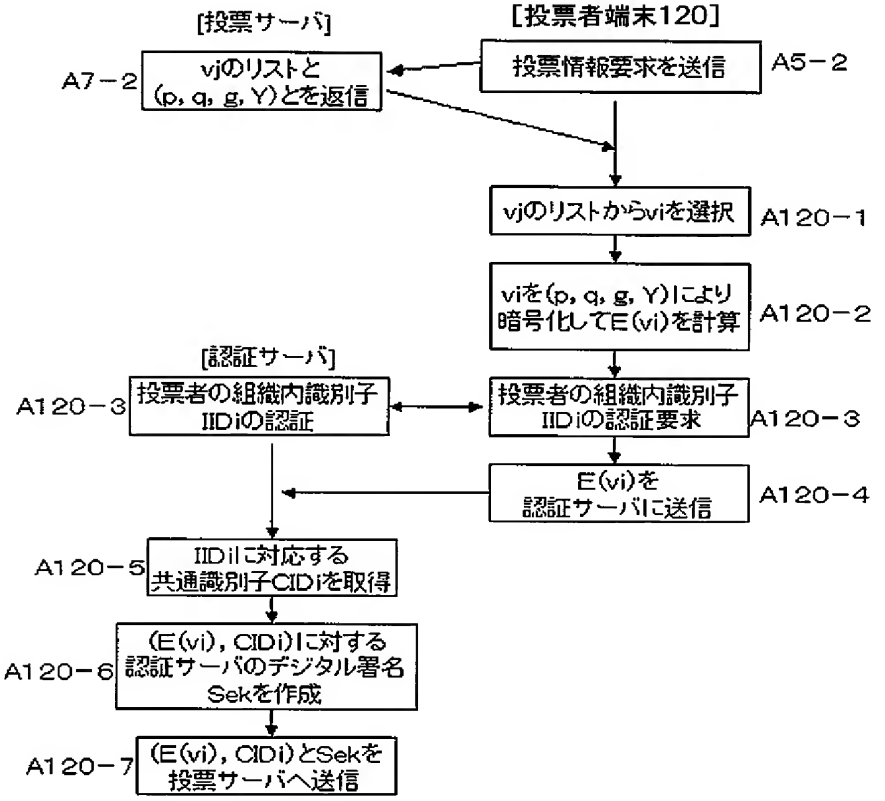
[図3]


[投票サーバ]
[投票者端末100]
すべての候補者名vjを(p, q, g, Y)で暗号化して(vj, E(vj))のリストを作成
A6
暗号投票情報要求を送信
A5−1
(vj, E(vj))のリストと(p, q, g, Y)とを返信
A7−1
[暗号サーバ400]
vjのリストからviを選択
A100−1
A100−3
Viに対応するE(Vi)と(p, q, g, Y)とを暗号サーバに送信
A100−2
E(vi)を(p, q, g, Y)により再度暗号化してE'(vi)を計算
E'(vi)を投票者端末に返信
A100−4
[認証サーバ]
投票者の組織内識別子IIDiの認証
A100−5
投票者の組織内識別子IIDiの認証要求
A100−5
E'(vi)を認証サーバに送信
A100−6
IIDiに対応する共通識別子CIDiを取得
A100−7
(E'(vi), CIDi)に対する認証サーバのデジタル署名Sekを作成
A100−8
(E'(vi), CIDi)とSekを投票サーバへ送信
A100−9

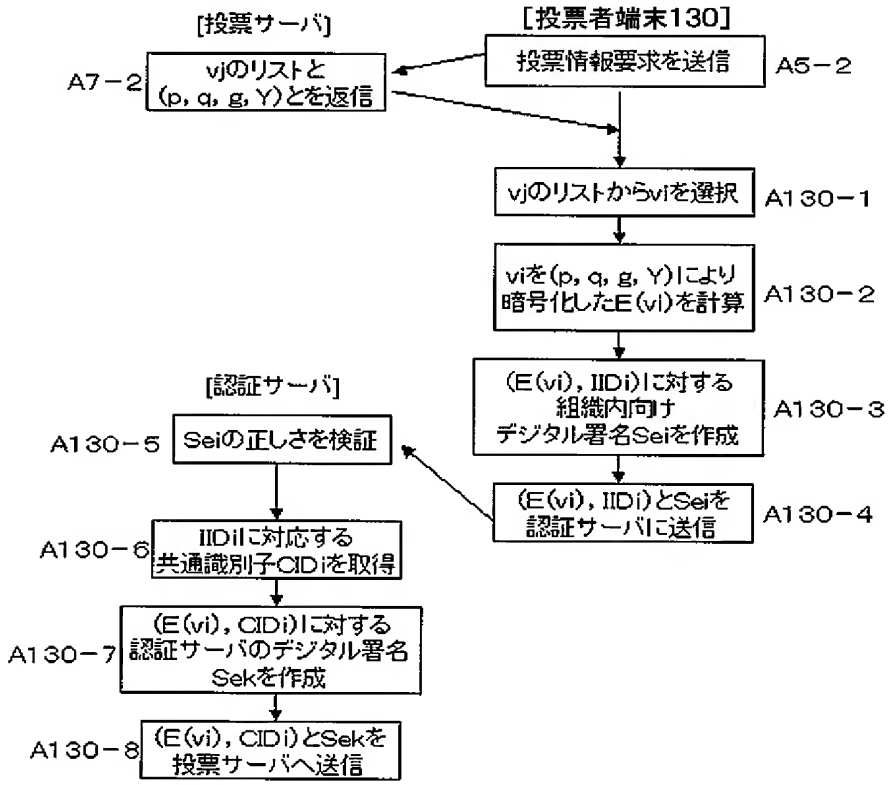
[図4]


[投票サーバ]
[投票者端末110]
すべての候補者名vjを(p, q, g, Y)で暗号化して(vj, E(vj))のリストを作成
A6
暗号投票情報要求を送信
A5−1
(vj, E(vj))のリストと(p, q, g, Y)とを返信
A7−1
[暗号サーバ410]
vjのリストからviを選択
A110−1
A110−3
Viに対応するE(Vi)と(p, q, g, Y)とを暗号サーバに送信
A110−2
E(vi)を(p, q, g, Y)により再度暗号化してE'(vi)を計算
E'(vi)を投票者端末に返信
A110−4
[認証サーバ]
(E'(vi), IIDi)に対する組織内向けデジタル署名Seiを作成
A110−5
Seiの正しさを検証
A110−7
(E'(vi), IIDi)とSeiを認証サーバに送信
A110−6
IIDiに対応する共通識別子CIDiを取得
A110−8
(E'(vi), CIDi)に対する認証サーバのデジタル署名Sekを作成
A110−9
(E'(vi), CIDi)とSekを投票サーバへ送信
A110−10

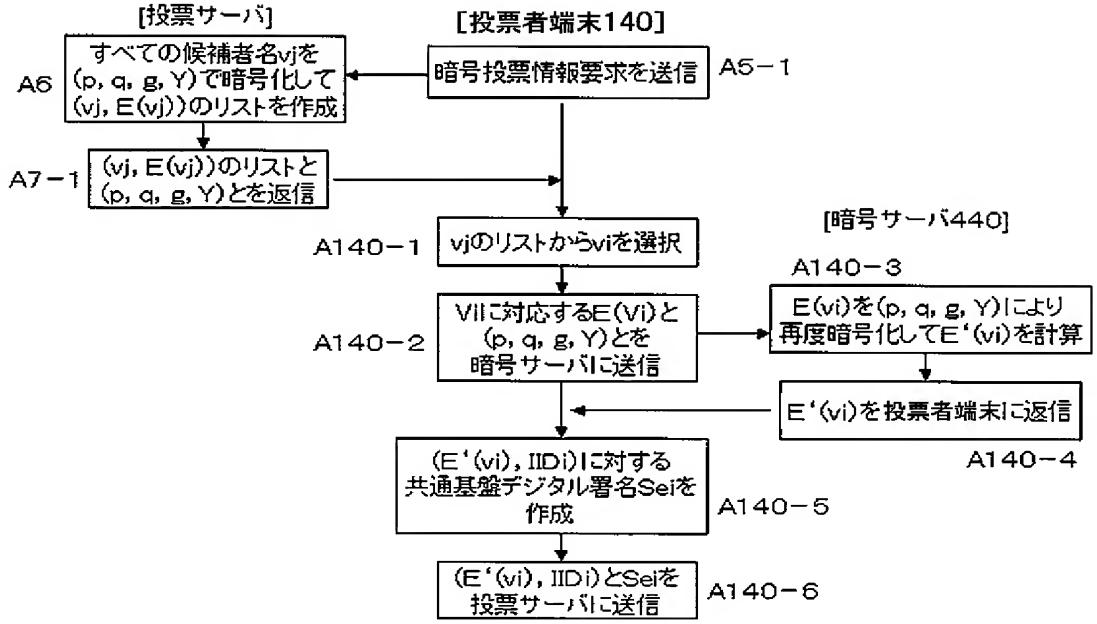
[図5]


[投票サーバ]
[投票者端末120]
A7－2
vjのリストと
(p, q, g, Y)とを返信
投票情報要求を送信
A5－2
vjのリストからviを選択
A120－1
viを(p, q, g, Y)により
暗号化してE(vi)を計算
A120－2
[認証サーバ]
A120－3
投票者の組織内識別子
IIDiの認証
投票者の組織内識別子
IIDiの認証要求
A120－3
E(vi)を
認証サーバに送信
A120－4
A120－5
IIDiに対応する
共通識別子CIDiを取得
A120－6
(E(vi), CIDi)に対する
認証サーバのデジタル署名
Sekを作成
A120－7
(E(vi), CIDi)とSekを
投票サーバへ送信

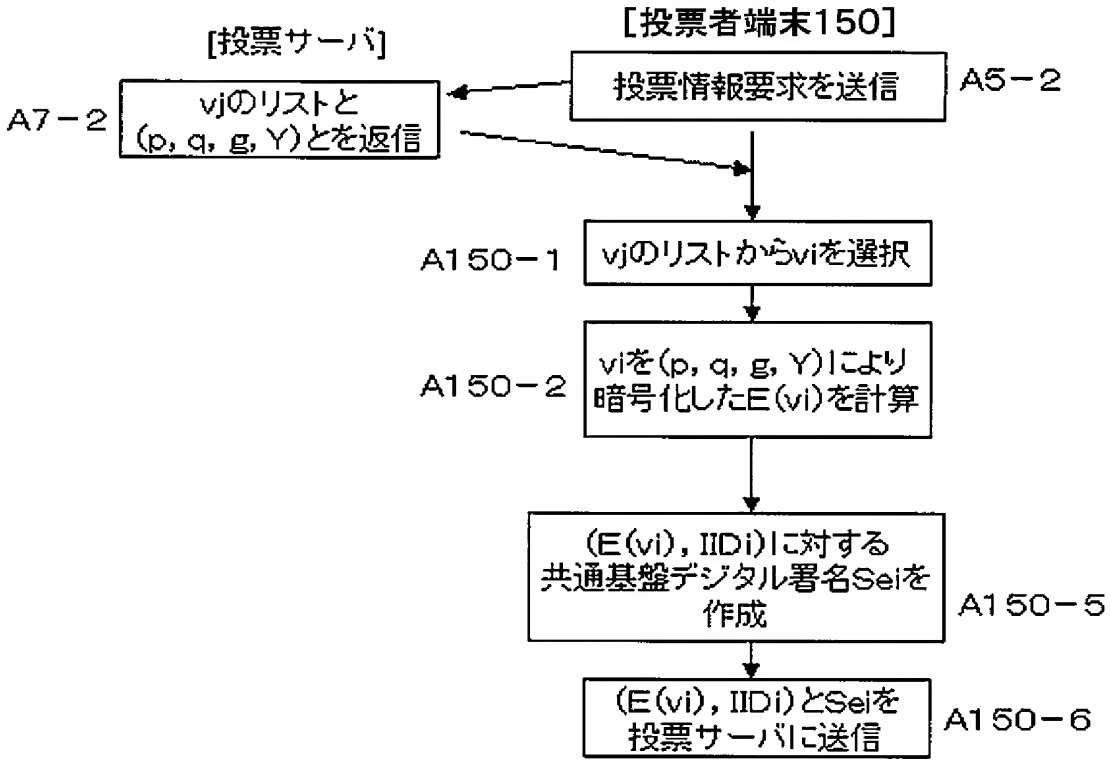
[図6]


[投票サーバ]
[投票者端末130]
A7－2
vjのリストと
(p, q, g, Y)とを返信
投票情報要求を送信
A5－2
vjのリストからviを選択
A130－1
viを(p, q, g, Y)により
暗号化したE(vi)を計算
A130－2
(E(vi), IIDi)に対する
組織内向け
デジタル署名Seiを作成
A130－3
[認証サーバ]
A130－5
Seiの正しさを検証
(E(vi), IIDi)とSeiを
認証サーバに送信
A130－4
A130－6
IIDiに対応する
共通識別子CIDiを取得
A130－7
(E(vi), CIDi)に対する
認証サーバのデジタル署名
Sekを作成
A130－8
(E(vi), CIDi)とSekを
投票サーバへ送信

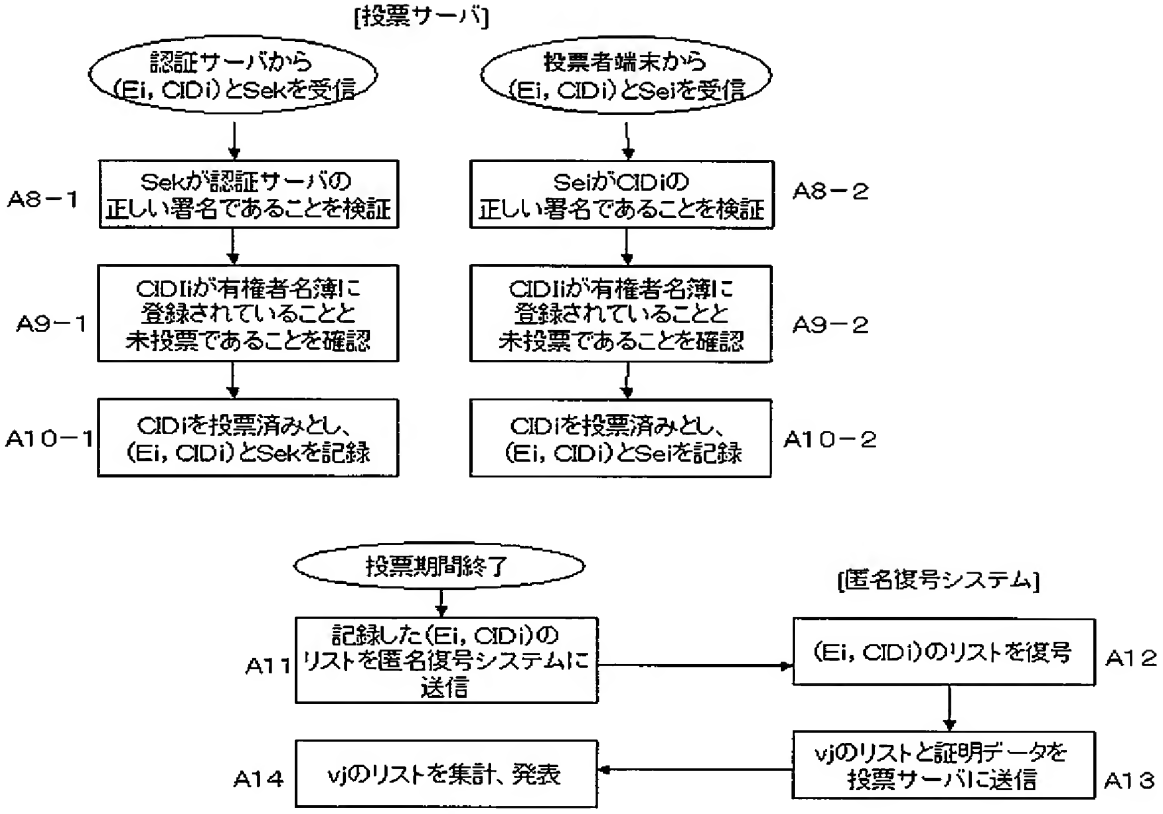
[図7]


[投票サーバ]
[投票者端末140]
すべての候補者名vjを(p, q, g, Y)で暗号化して(vj, E(vj))のリストを作成
A6
暗号投票情報要求を送信
A5−1
(vj, E(vj))のリストと(p, q, g, Y)とを返信
A7−1
[暗号サーバ440]
A140−1
vjのリストからviを選択
A140−3
E(vi)を(p, q, g, Y)により再度暗号化してE'(vi)を計算
A140−2
Viに対応するE(Vi)と(p, q, g, Y)とを暗号サーバに送信
E'(vi)を投票者端末に返信
A140−4
(E'(vi), IIDi)に対する共通基盤デジタル署名Seiを作成
A140−5
(E'(vi), IIDi)とSeiを投票サーバに送信
A140−6

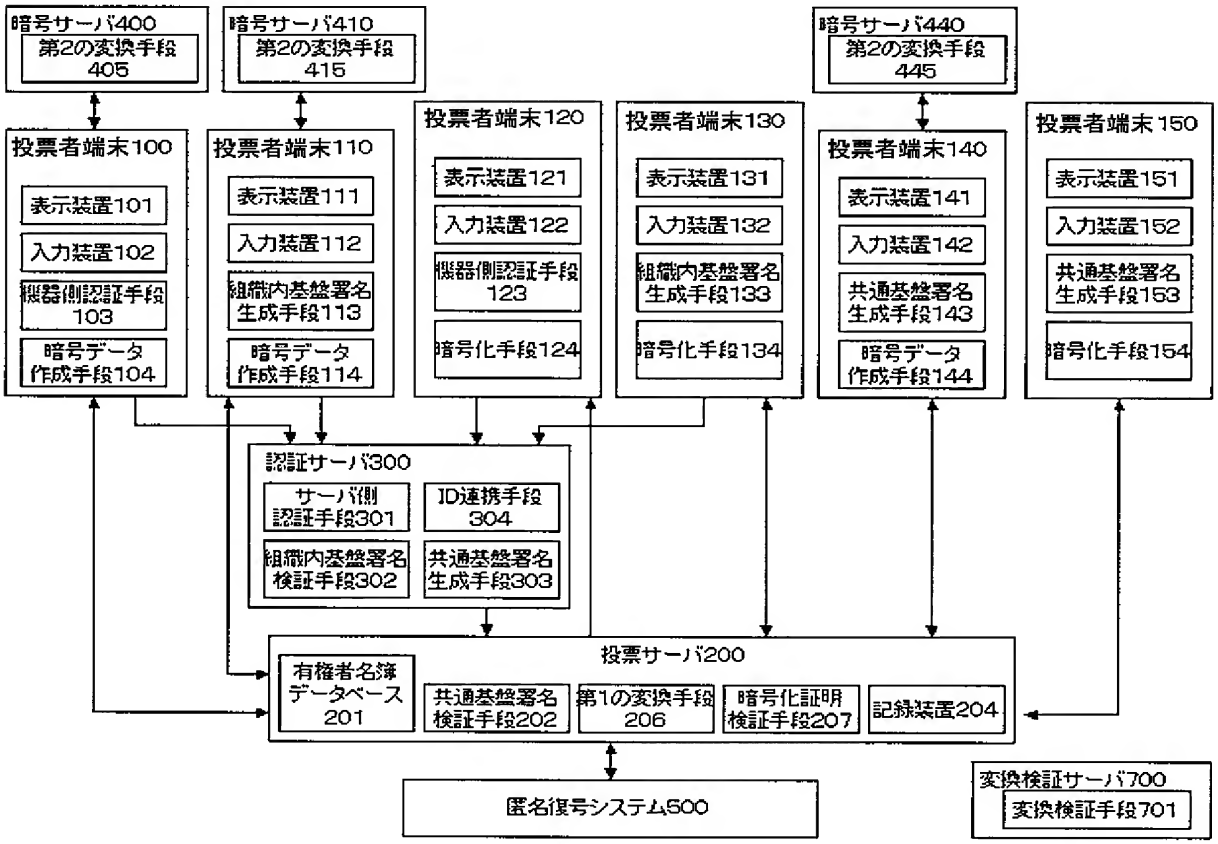
[図8]


[投票者端末150]
[投票サーバ]
投票情報要求を送信
A5−2
vjのリストと(p, q, g, Y)とを返信
A7−2
A150−1
vjのリストからviを選択
A150−2
viを(p, q, g, Y)により暗号化したE(vi)を計算
(E(vi), IIDi)に対する共通基盤デジタル署名Seiを作成
A150−5
(E(vi), IIDi)とSeiを投票サーバに送信
A150−6

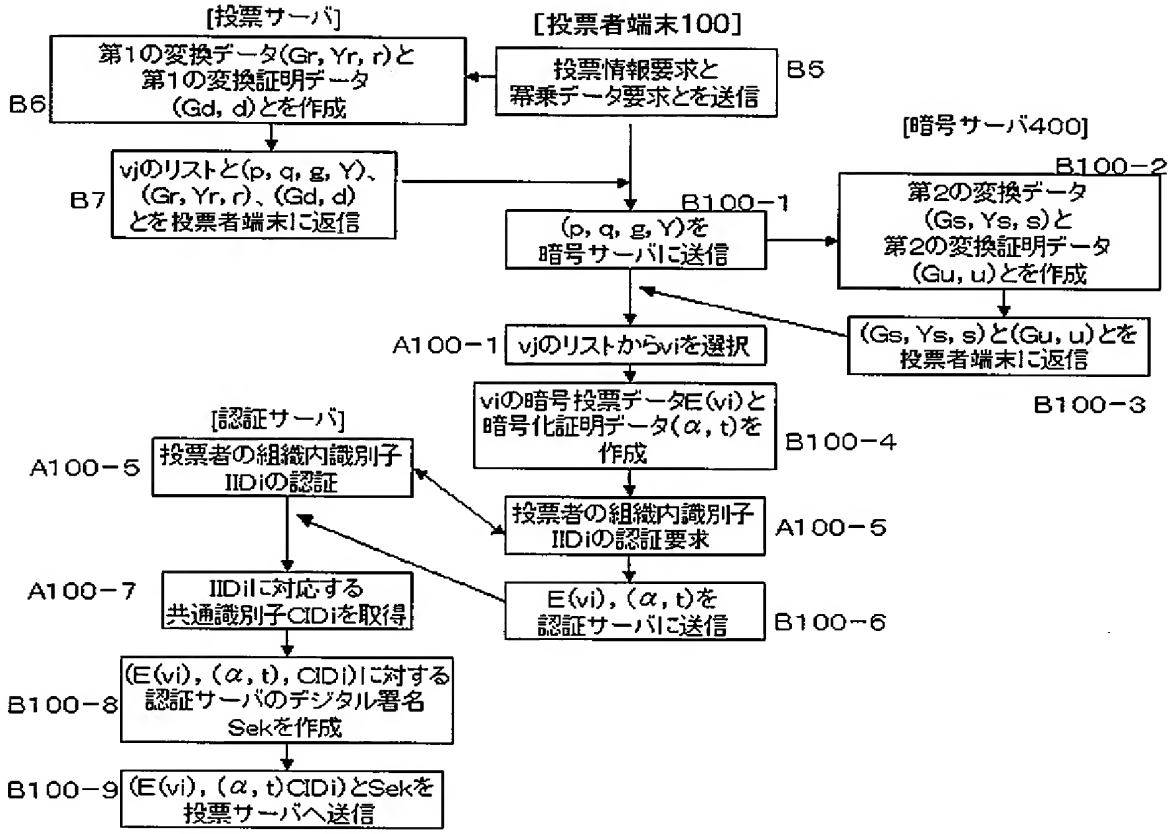
[図9]


[投票サーバ]
認証サーバから (Ei, CIDi)とSekを受信
投票者端末から (Ei, CIDi)とSeiを受信
A8−1
Sekが認証サーバの正しい署名であることを検証
SeiがCIDiの正しい署名であることを検証
A8−2
A9−1
CIDiが有権者名簿に登録されていることと未投票であることを確認
CIDiが有権者名簿に登録されていることと未投票であることを確認
A9−2
A10−1
CIDiを投票済みとし、(Ei, CIDi)とSekを記録
CIDiを投票済みとし、(Ei, CIDi)とSeiを記録
A10−2
投票期間終了
[匿名復号システム]
A11
記録した(Ei, CIDi)のリストを匿名復号システムに送信
(Ei, CIDi)のリストを復号
A12
vjのリストと証明データを投票サーバに送信
A13
A14
vjのリストを集計、発表

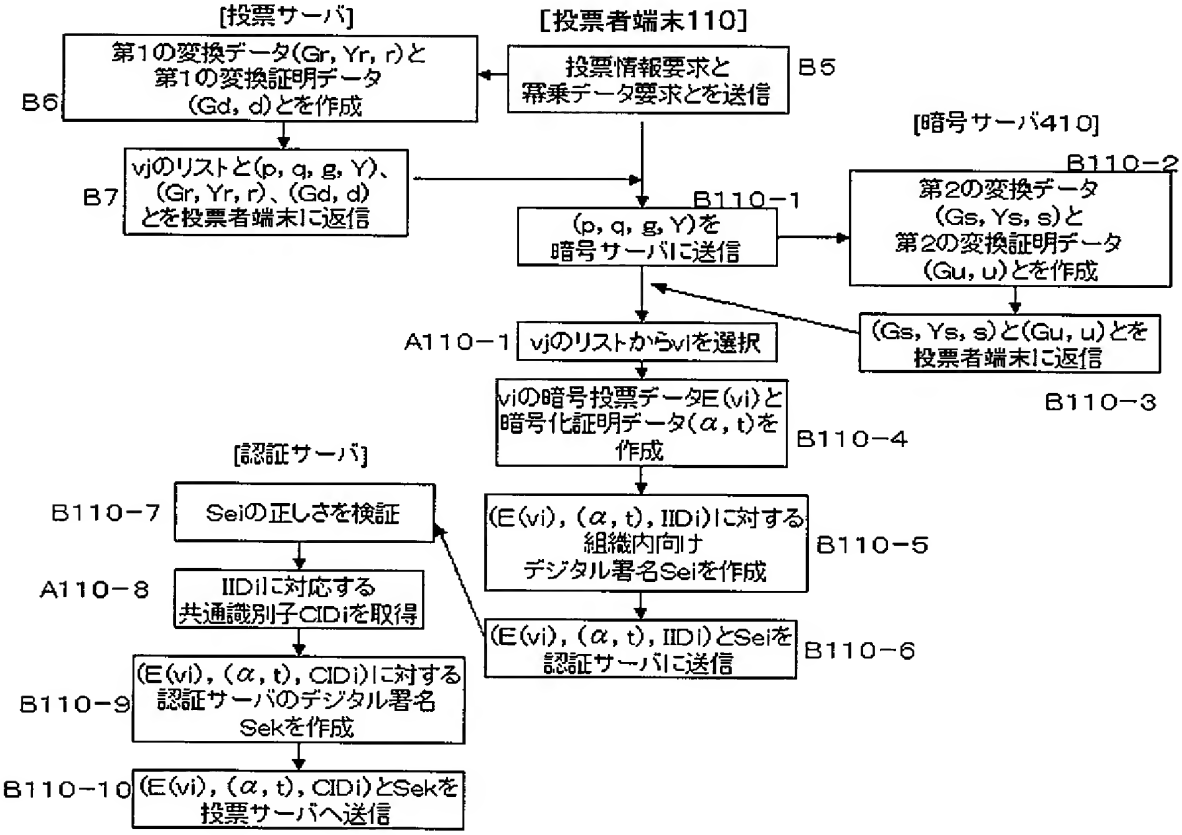
[図10]


暗号サーバ400
第2の変換手段405
暗号サーバ410
第2の変換手段415
暗号サーバ440
第2の変換手段445
投票者端末100
表示装置101
入力装置102
機器側認証手段103
暗号データ作成手段104
投票者端末110
表示装置111
入力装置112
組織内基盤署名生成手段113
暗号データ作成手段114
投票者端末120
表示装置121
入力装置122
機器側認証手段123
暗号化手段124
投票者端末130
表示装置131
入力装置132
組織内基盤署名生成手段133
暗号化手段134
投票者端末140
表示装置141
入力装置142
共通基盤署名生成手段143
暗号データ作成手段144
投票者端末150
表示装置151
入力装置152
共通基盤署名生成手段153
暗号化手段154
認証サーバ300
サーバ側認証手段301
ID連携手段304
組織内基盤署名検証手段302
共通基盤署名生成手段303
投票サーバ200
有権者名簿データベース201
共通基盤署名検証手段202
第1の変換手段206
暗号化証明検証手段207
記録装置204
匿名復号システム500
変換検証サーバ700
変換検証手段701

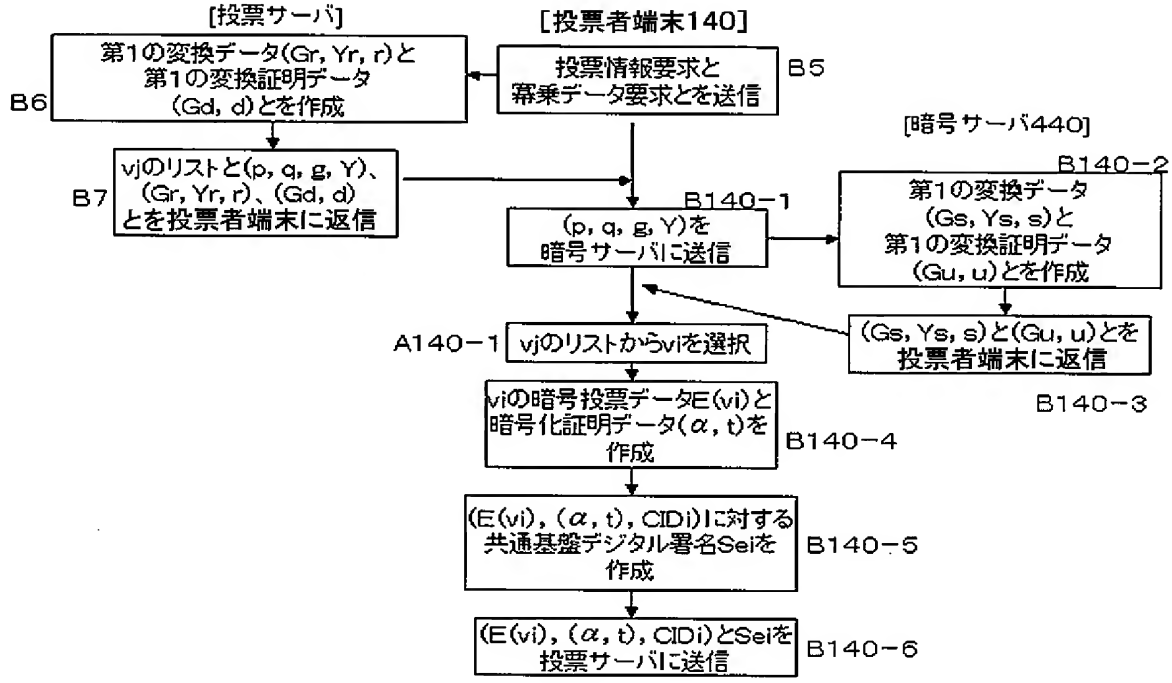
[図11]


[投票サーバ]
[投票者端末100]
第1の変換データ(Gr, Yr, r)と第1の変換証明データ(Gd, d)とを作成
B6
投票情報要求と冪乗データ要求とを送信
B5
vjのリストと(p, q, g, Y)、(Gr, Yr, r)、(Gd, d)とを投票者端末に返信
B7
[暗号サーバ400]
B100-2
(p, q, g, Y)を暗号サーバに送信
B100-1
第2の変換データ(Gs, Ys, s)と第2の変換証明データ(Gu, u)とを作成
(Gs, Ys, s)と(Gu, u)とを投票者端末に返信
B100-3
A100-1
vjのリストからviを選択
viの暗号投票データE(vi)と暗号化証明データ(α, t)を作成
B100-4
[認証サーバ]
A100-5
投票者の組織内識別子IIDiの認証
投票者の組織内識別子IIDiの認証要求
A100-5
A100-7
IIDiに対応する共通識別子CIDiを取得
E(vi), (α, t)を認証サーバに送信
B100-6
(E(vi), (α, t), CIDi)に対する認証サーバのデジタル署名Sekを作成
B100-8
B100-9
(E(vi), (α, t)CIDi)とSekを投票サーバへ送信

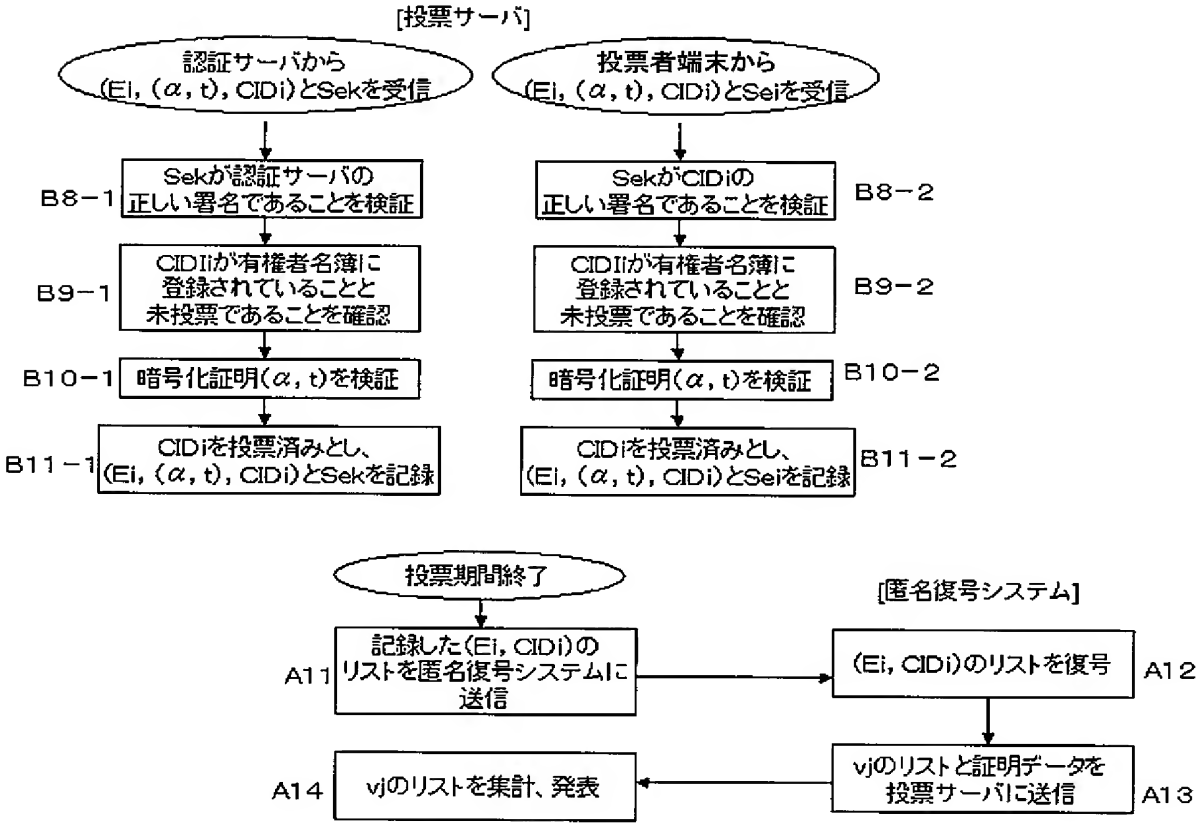
[図12]


[投票サーバ]
[投票者端末110]
第1の変換データ(Gr, Yr, r)と第1の変換証明データ(Gd, d)とを作成
B6
投票情報要求と冪乗データ要求とを送信
B5
vjのリストと(p, q, g, Y)、(Gr, Yr, r)、(Gd, d)とを投票者端末に返信
B7
[暗号サーバ410]
B110-2
(p, q, g, Y)を暗号サーバに送信
B110-1
第2の変換データ(Gs, Ys, s)と第2の変換証明データ(Gu, u)とを作成
(Gs, Ys, s)と(Gu, u)とを投票者端末に返信
B110-3
A110-1
vjのリストからviを選択
viの暗号投票データE(vi)と暗号化証明データ(α, t)を作成
B110-4
[認証サーバ]
B110-7
Seiの正しさを検証
(E(vi), (α, t), IIDi)に対する組織内向けデジタル署名Seiを作成
B110-5
A110-8
IIDiに対応する共通識別子CIDiを取得
(E(vi), (α, t), IIDi)とSeiを認証サーバに送信
B110-6
(E(vi), (α, t), CIDi)に対する認証サーバのデジタル署名Sekを作成
B110-9
B110-10
(E(vi), (α, t), CIDi)とSekを投票サーバへ送信

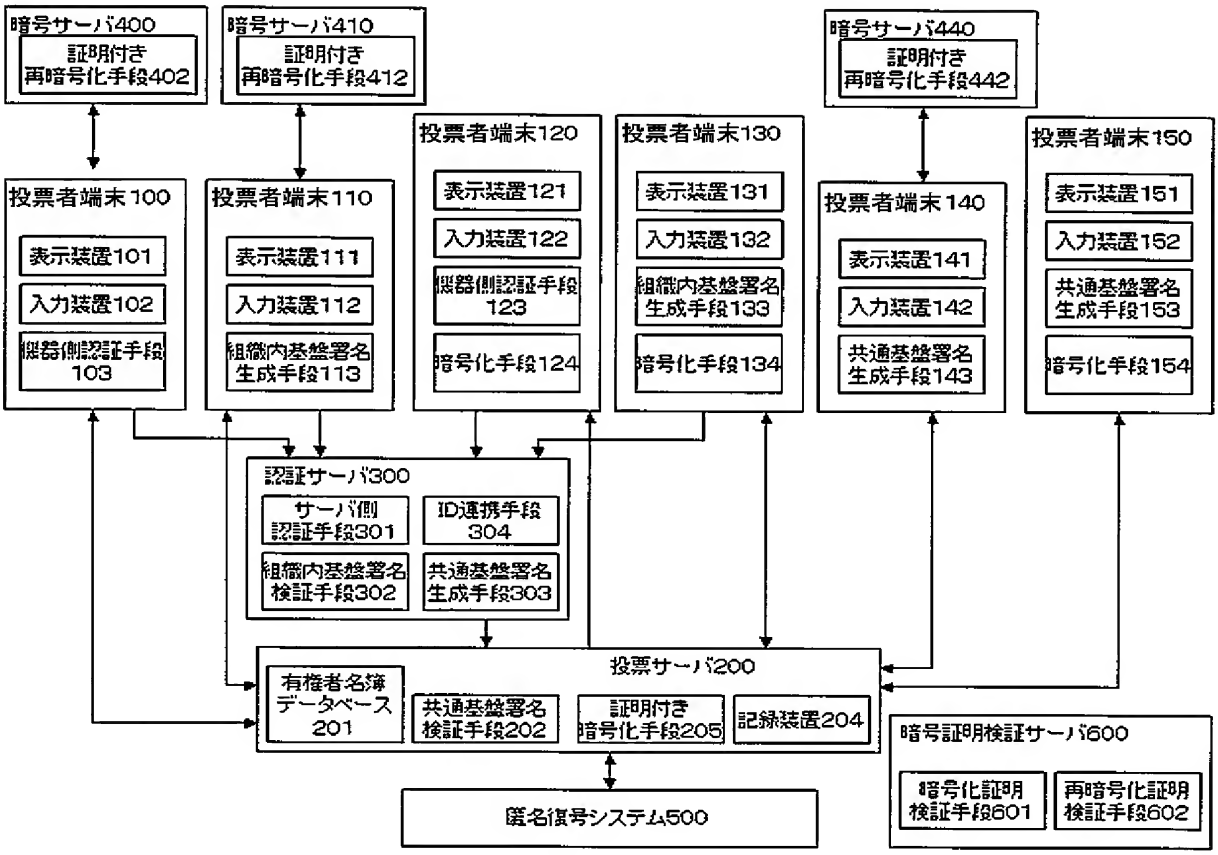
[図13]


[投票サーバ]
[投票者端末140]
第1の変換データ(Gr, Yr, r)と
第1の変換証明データ
(Gd, d)とを作成
B6
投票情報要求と
冪乗データ要求とを送信
B5
[暗号サーバ440]
vjのリストと(p, q, g, Y)、
(Gr, Yr, r)、(Gd, d)
とを投票者端末に返信
B7
B140−1
(p, q, g, Y)を
暗号サーバに送信
B140−2
第1の変換データ
(Gs, Ys, s)と
第1の変換証明データ
(Gu, u)とを作成
(Gs, Ys, s)と(Gu, u)とを
投票者端末に返信
B140−3
A140−1
vjのリストからviを選択
viの暗号投票データE(vi)と
暗号化証明データ(α, t)を
作成
B140−4
(E(vi), (α, t), CIDi)に対する
共通基盤デジタル署名Seiを
作成
B140−5
(E(vi), (α, t), CIDi)とSeiを
投票サーバに送信
B140−6

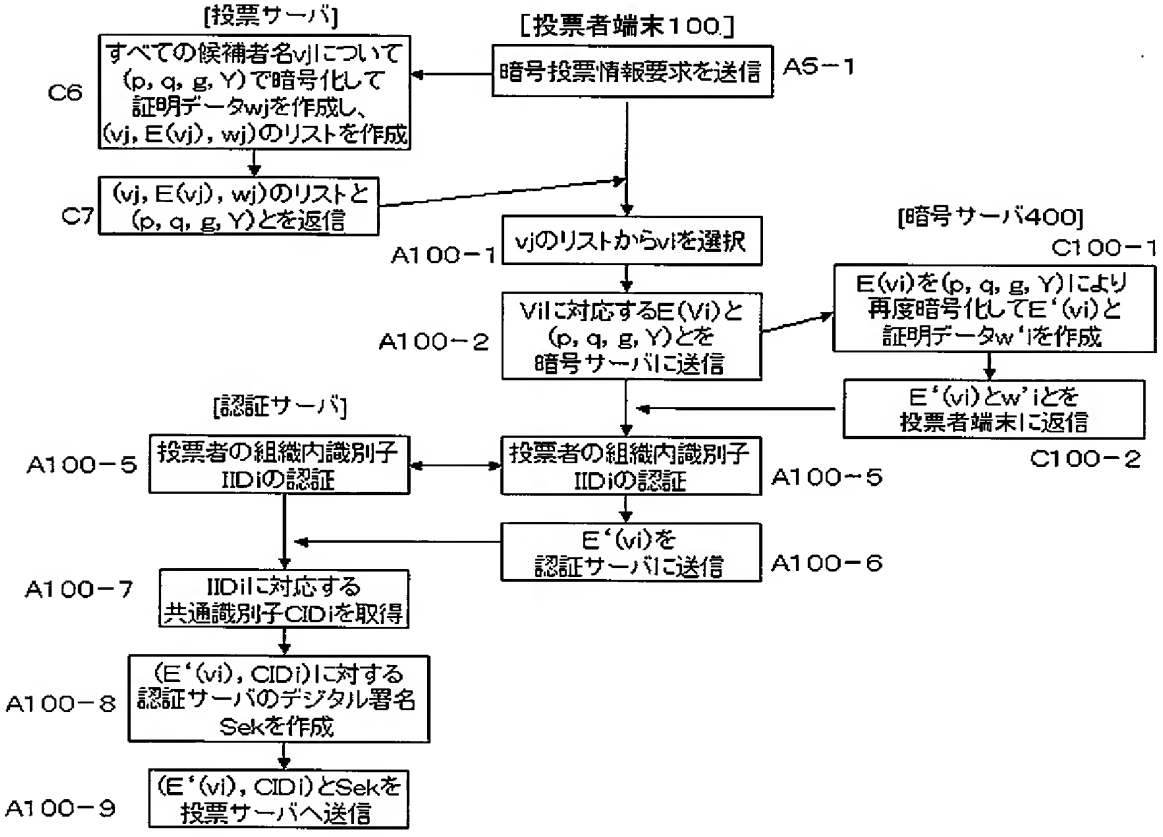
[図14]


[投票サーバ]
認証サーバから
(Ei, (α, t), CIDi)とSekを受信
投票者端末から
(Ei, (α, t), CIDi)とSeiを受信
B8−1
Sekが認証サーバの
正しい署名であることを検証
SekがCIDiの
正しい署名であることを検証
B8−2
B9−1
CIDiiが有権者名簿に
登録されていることと
未投票であることを確認
CIDiiが有権者名簿に
登録されていることと
未投票であることを確認
B9−2
B10−1
暗号化証明(α, t)を検証
暗号化証明(α, t)を検証
B10−2
B11−1
CIDiを投票済みとし、
(Ei, (α, t), CIDi)とSekを記録
CIDiを投票済みとし、
(Ei, (α, t), CIDi)とSeiを記録
B11−2
投票期間終了
[匿名復号システム]
A11
記録した(Ei, CIDi)の
リストを匿名復号システムに
送信
(Ei, CIDi)のリストを復号
A12
A14
vjのリストを集計、発表
vjのリストと証明データを
投票サーバに送信
A13

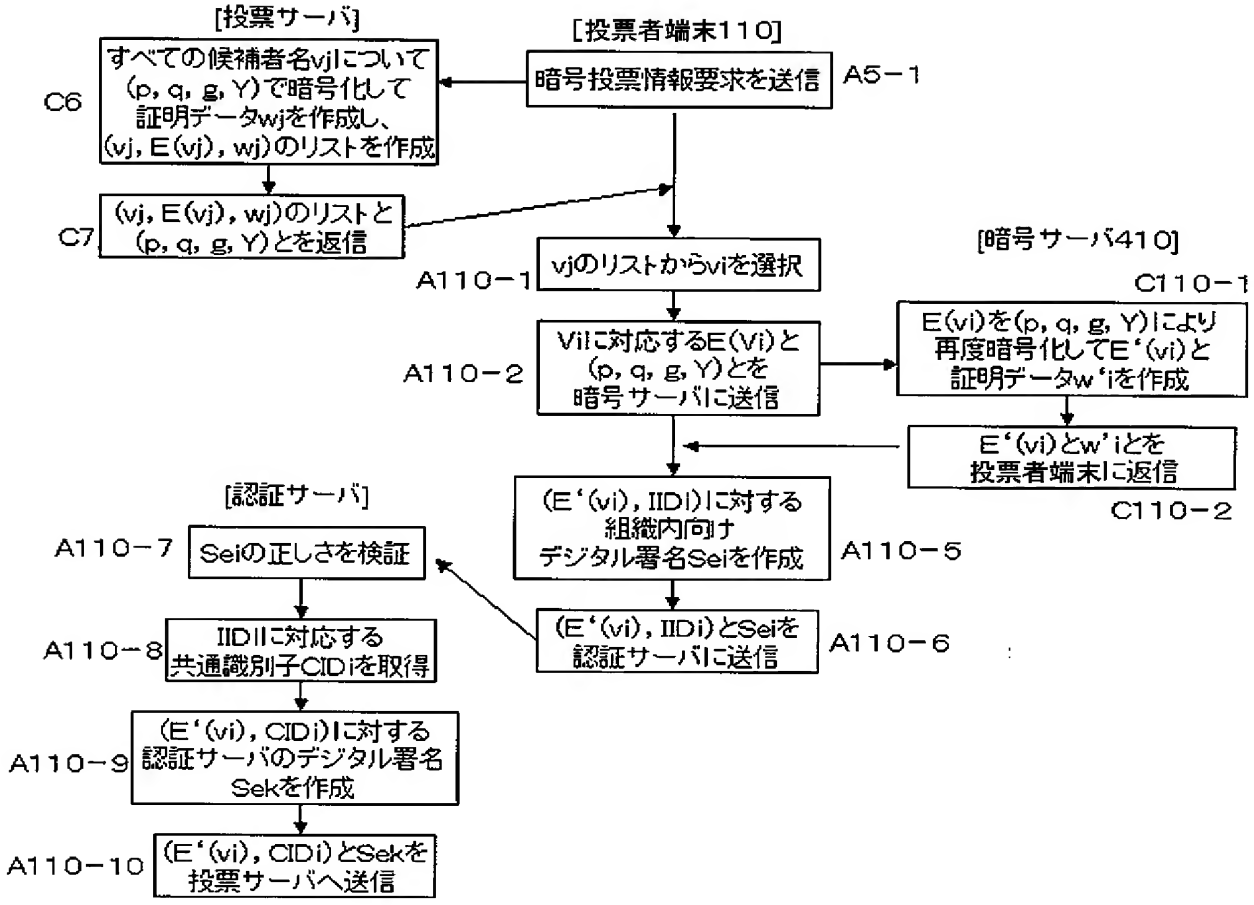
[図15]


暗号サーバ400
証明付き再暗号化手段402
暗号サーバ410
証明付き再暗号化手段412
暗号サーバ440
証明付き再暗号化手段442
投票者端末100
表示装置101
入力装置102
機器側認証手段103
投票者端末110
表示装置111
入力装置112
組織内基盤署名生成手段113
投票者端末120
表示装置121
入力装置122
機器側認証手段123
暗号化手段124
投票者端末130
表示装置131
入力装置132
組織内基盤署名生成手段133
暗号化手段134
投票者端末140
表示装置141
入力装置142
共通基盤署名生成手段143
投票者端末150
表示装置151
入力装置152
共通基盤署名生成手段153
暗号化手段154
認証サーバ300
サーバ側認証手段301
ID連携手段304
組織内基盤署名検証手段302
共通基盤署名生成手段303
投票サーバ200
有権者名簿データベース201
共通基盤署名検証手段202
証明付き暗号化手段205
記録装置204
暗号証明検証サーバ600
暗号化証明検証手段601
再暗号化証明検証手段602
匿名復号システム500

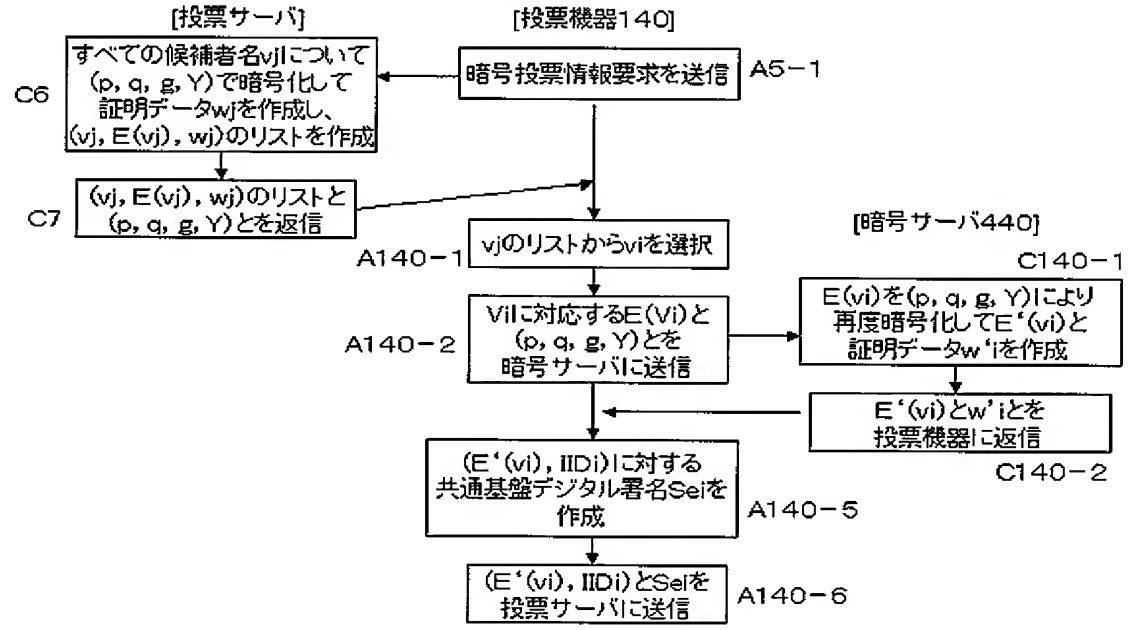
[図16]


[投票サーバ]
[投票者端末100]
C6
すべての候補者名vjについて(p, q, g, Y)で暗号化して証明データwjを作成し、(vj, E(vj), wj)のリストを作成
暗号投票情報要求を送信
A5−1
C7
(vj, E(vj), wj)のリストと(p, q, g, Y)とを返信
A100−1
vjのリストからviを選択
[暗号サーバ400]
C100−1
A100−2
Viに対応するE(Vi)と(p, q, g, Y)とを暗号サーバに送信
E(vi)を(p, q, g, Y)により再度暗号化してE'(vi)と証明データw'iを作成
E'(vi)とw'iとを投票者端末に返信
C100−2
[認証サーバ]
A100−5
投票者の組織内識別子IIDiの認証
投票者の組織内識別子IIDiの認証
A100−5
E'(vi)を認証サーバに送信
A100−6
A100−7
IIDiに対応する共通識別子CIDiを取得
A100−8
(E'(vi), CIDi)に対する認証サーバのデジタル署名Sekを作成
A100−9
(E'(vi), CIDi)とSekを投票サーバへ送信

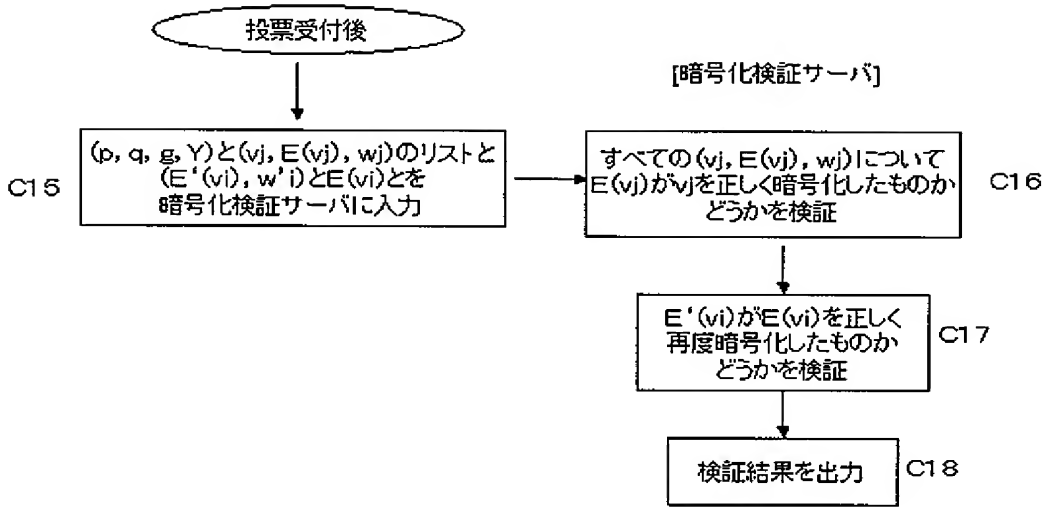
[図17]


[投票サーバ]
[投票者端末110]
すべての候補者名vjについて(p, q, g, Y)で暗号化して証明データwjを作成し、(vj, E(vj), wj)のリストを作成
C6
暗号投票情報要求を送信
A5−1
(vj, E(vj), wj)のリストと(p, q, g, Y)とを返信
C7
vjのリストからviを選択
A110−1
[暗号サーバ410]
C110−1
Viに対応するE(Vi)と(p, q, g, Y)とを暗号サーバに送信
A110−2
E(vi)を(p, q, g, Y)により再度暗号化してE'(vi)と証明データw'iを作成
E'(vi)とw'iとを投票者端末に返信
C110−2
(E'(vi), IIDi)に対する組織内向けデジタル署名Seiを作成
A110−5
[認証サーバ]
Seiの正しさを検証
A110−7
(E'(vi), IIDi)とSeiを認証サーバに送信
A110−6
IIDiに対応する共通識別子CIDiを取得
A110−8
(E'(vi), CIDi)に対する認証サーバのデジタル署名Sekを作成
A110−9
(E'(vi), CIDi)とSekを投票サーバへ送信
A110−10

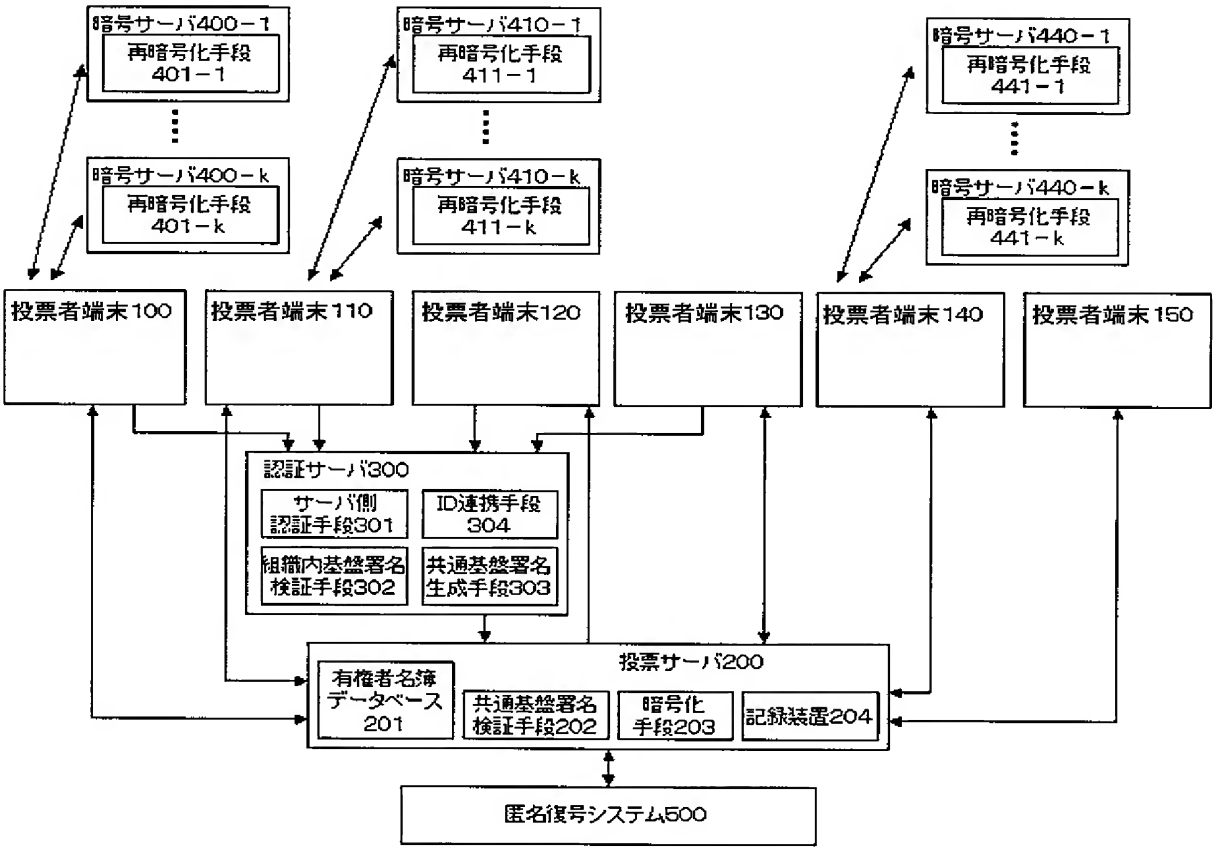
[図18]


[投票サーバ]
[投票機器140]
すべての候補者名vjについて(p, q, g, Y)で暗号化して証明データwjを作成し、(vj, E(vj), wj)のリストを作成
C6
暗号投票情報要求を送信
A5−1
(vj, E(vj), wj)のリストと(p, q, g, Y)とを返信
C7
vjのリストからviを選択
A140−1
[暗号サーバ440]
C140−1
Viに対応するE(Vi)と(p, q, g, Y)とを暗号サーバに送信
A140−2
E(vi)を(p, q, g, Y)により再度暗号化してE'(vi)と証明データw'iを作成
E'(vi)とw'iとを投票機器に返信
C140−2
(E'(vi), IIDi)に対する共通基盤デジタル署名Seiを作成
A140−5
(E'(vi), IIDi)とSeiを投票サーバに送信
A140−6

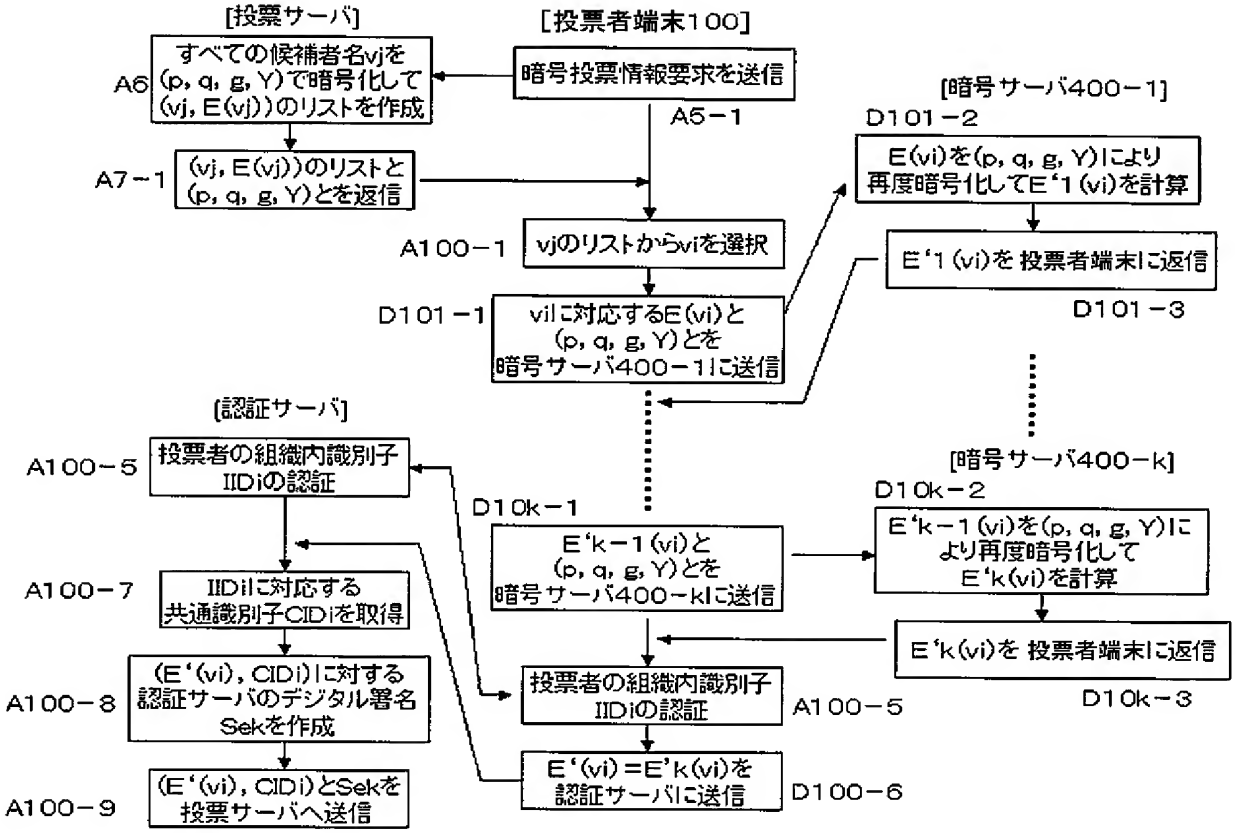
[図19]


投票受付後
[暗号化検証サーバ]
C15
(p, q, g, Y)と(vj, E(vj), wj)のリストと
(E'(vi), w'i)とE(vi)とを
暗号化検証サーバに入力
すべての(vj, E(vj), wj)について
E(vj)がvjを正しく暗号化したものか
どうかを検証
C16
E'(vi)がE(vi)を正しく
再度暗号化したものか
どうかを検証
C17
検証結果を出力
C18

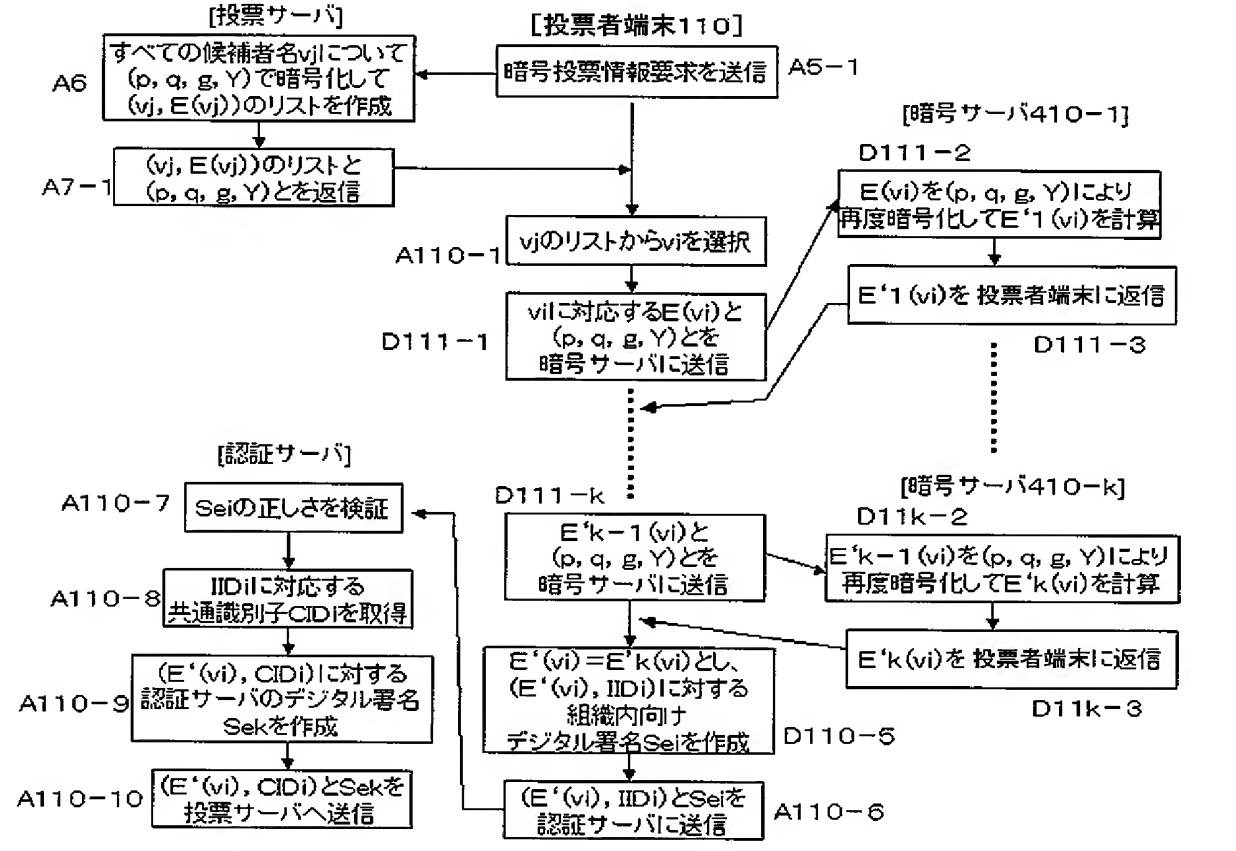
[図20]


暗号サーバ400－1
再暗号化手段
401－1
暗号サーバ400－k
再暗号化手段
401－k
暗号サーバ410－1
再暗号化手段
411－1
暗号サーバ410－k
再暗号化手段
411－k
暗号サーバ440－1
再暗号化手段
441－1
暗号サーバ440－k
再暗号化手段
441－k
投票者端末100
投票者端末110
投票者端末120
投票者端末130
投票者端末140
投票者端末150
認証サーバ300
サーバ側
認証手段301
ID連携手段
304
組織内基盤署名
検証手段302
共通基盤署名
生成手段303
投票サーバ200
有権者名簿
データベース
201
共通基盤署名
検証手段202
暗号化
手段203
記録装置204
匿名復号システム500

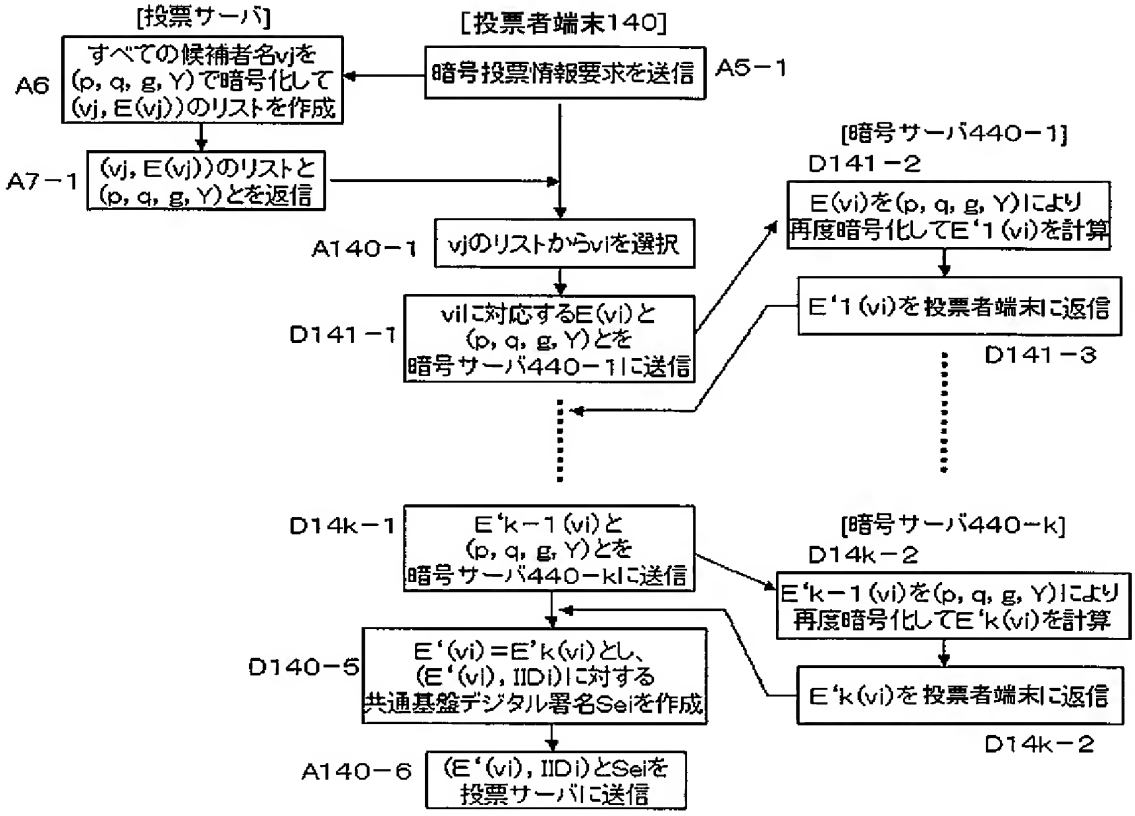
[図21]


[投票サーバ]
[投票者端末100]
すべての候補者名vjを(p, q, g, Y)で暗号化して(vj, E(vj))のリストを作成
A6
暗号投票情報要求を送信
A5−1
(vj, E(vj))のリストと(p, q, g, Y)とを返信
A7−1
[暗号サーバ400−1]
D101−2
E(vi)を(p, q, g, Y)により再度暗号化してE'1(vi)を計算
E'1(vi)を投票者端末に返信
D101−3
vjのリストからviを選択
A100−1
viに対応するE(vi)と(p, q, g, Y)とを暗号サーバ400−1に送信
D101−1
[認証サーバ]
投票者の組織内識別子IIDiの認証
A100−5
[暗号サーバ400−k]
D10k−2
E'k−1(vi)を(p, q, g, Y)により再度暗号化してE'k(vi)を計算
D10k−1
E'k−1(vi)と(p, q, g, Y)とを暗号サーバ400−kに送信
IIDiに対応する共通識別子CIDiを取得
A100−7
E'k(vi)を投票者端末に返信
D10k−3
(E'(vi), CIDi)に対する認証サーバのデジタル署名Sekを作成
A100−8
投票者の組織内識別子IIDiの認証
A100−5
(E'(vi), CIDi)とSekを投票サーバへ送信
A100−9
E'(vi)=E'k(vi)を認証サーバに送信
D100−6

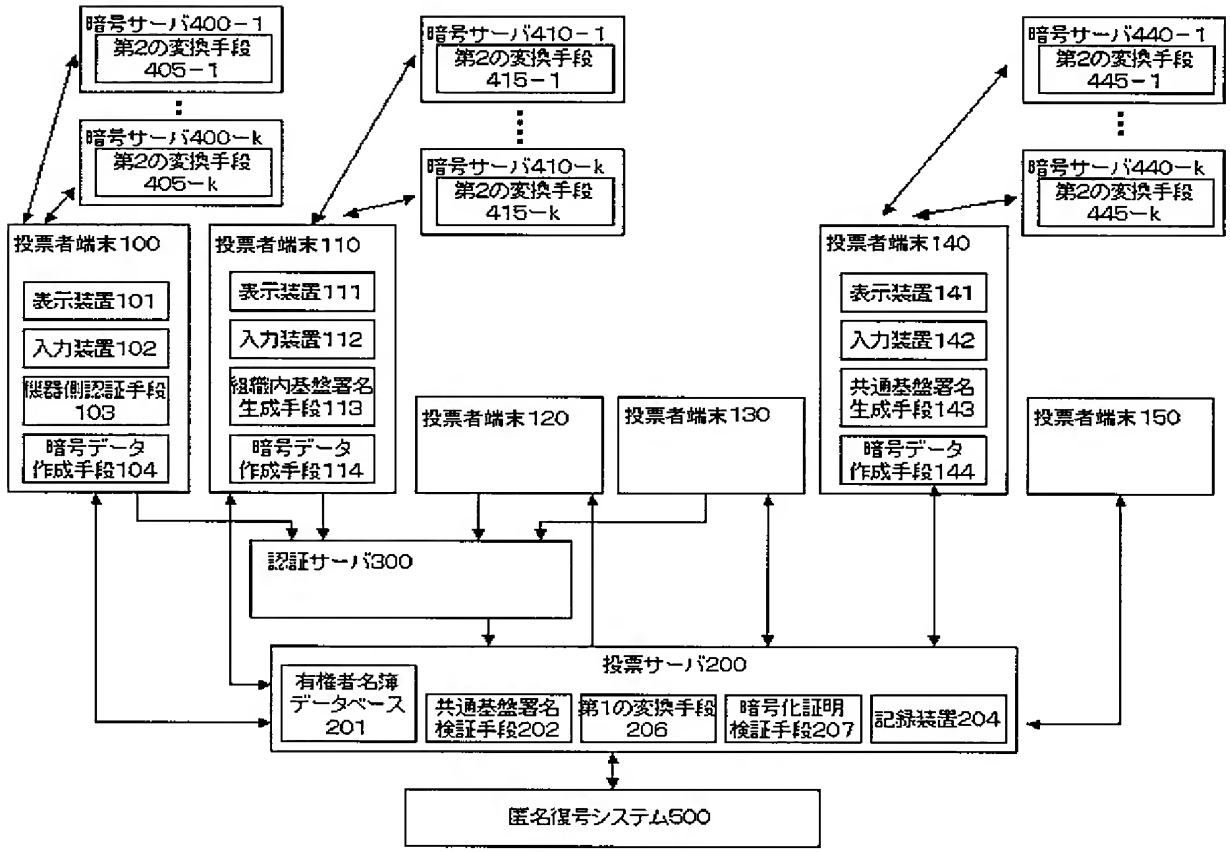
[図22]


[投票サーバ]
[投票者端末110]
すべての候補者名vjについて(p, q, g, Y)で暗号化して(vj, E(vj))のリストを作成
A6
暗号投票情報要求を送信
A5−1
(vj, E(vj))のリストと(p, q, g, Y)とを返信
A7−1
[暗号サーバ410−1]
D111−2
E(vi)を(p, q, g, Y)により再度暗号化してE'1(vi)を計算
E'1(vi)を投票者端末に返信
D111−3
vjのリストからviを選択
A110−1
viに対応するE(vi)と(p, q, g, Y)とを暗号サーバに送信
D111−1
[認証サーバ]
Seiの正しさを検証
A110−7
[暗号サーバ410−k]
D111−k
D11k−2
E'k−1(vi)と(p, q, g, Y)とを暗号サーバに送信
E'k−1(vi)を(p, q, g, Y)により再度暗号化してE'k(vi)を計算
IIDiに対応する共通識別子CIDiを取得
A110−8
E'k(vi)を投票者端末に返信
D11k−3
(E'(vi), CIDi)に対する認証サーバのデジタル署名Sekを作成
A110−9
E'(vi)=E'k(vi)とし、(E'(vi), IIDi)に対する組織内向けデジタル署名Seiを作成
D110−5
(E'(vi), CIDi)とSekを投票サーバへ送信
A110−10
(E'(vi), IIDi)とSeiを認証サーバに送信
A110−6

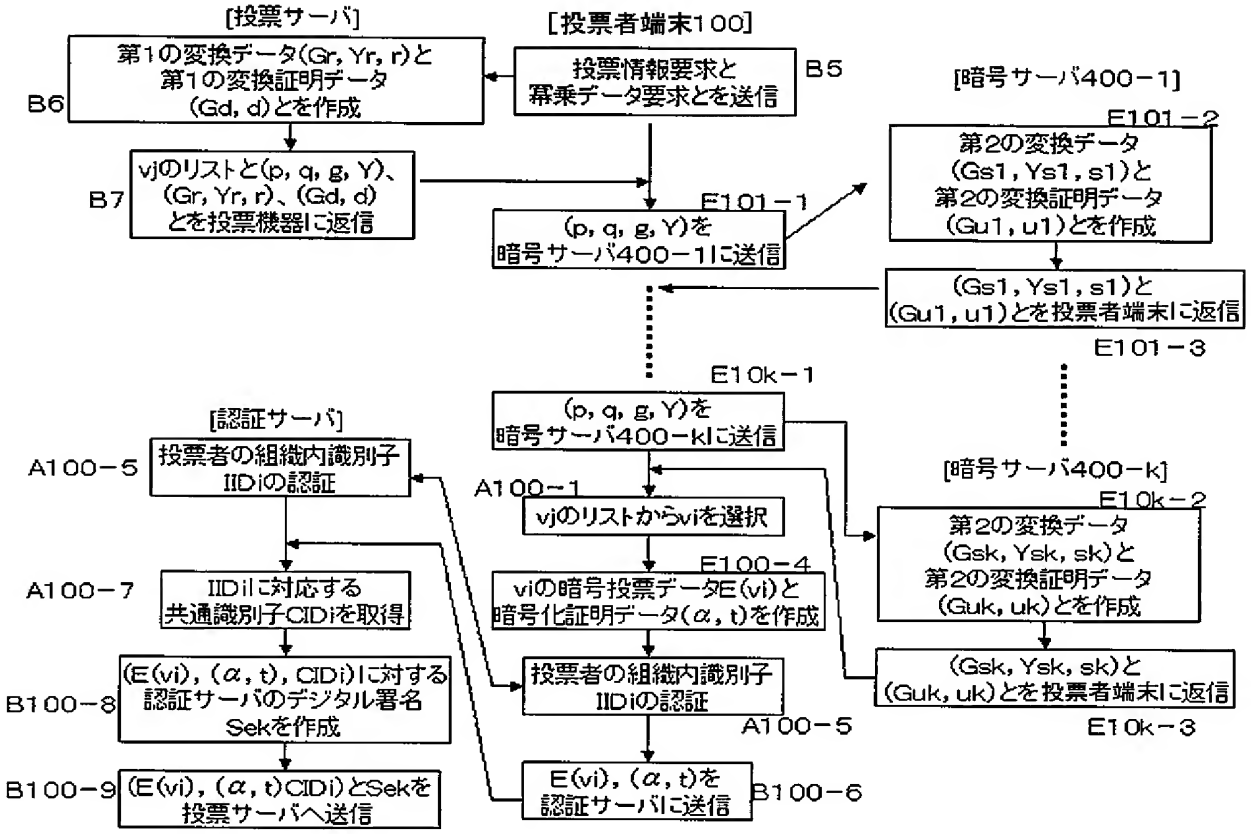
[図23]


[投票サーバ]
[投票者端末140]
すべての候補者名vjを(p, q, g, Y)で暗号化して(vj, E(vj))のリストを作成
A6
暗号投票情報要求を送信
A5−1
(vj, E(vj))のリストと(p, q, g, Y)とを返信
A7−1
vjのリストからviを選択
A140−1
viに対応するE(vi)と(p, q, g, Y)とを暗号サーバ440−1に送信
D141−1
[暗号サーバ440−1]
D141−2
E(vi)を(p, q, g, Y)により再度暗号化してE'1(vi)を計算
E'1(vi)を投票者端末に返信
D141−3
D14k−1
E'k−1(vi)と(p, q, g, Y)とを暗号サーバ440−kに送信
[暗号サーバ440−k]
D14k−2
E'k−1(vi)を(p, q, g, Y)により再度暗号化してE'k(vi)を計算
E'k(vi)を投票者端末に返信
D14k−2
D140−5
E'(vi)=E'k(vi)とし、(E'(vi), IIDi)に対する共通基盤デジタル署名Seiを作成
A140−6
(E'(vi), IIDi)とSeiを投票サーバに送信

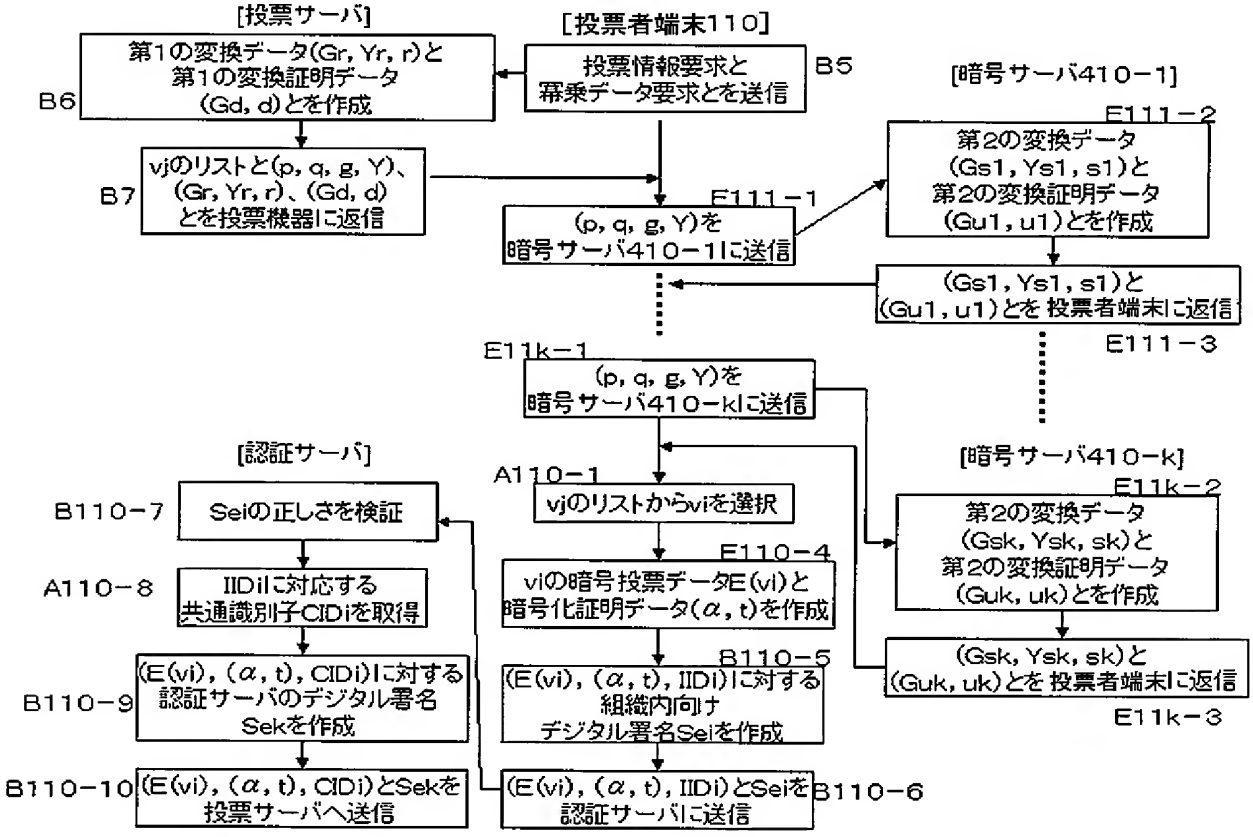
[図24]


暗号サーバ400−1
第2の変換手段405−1
暗号サーバ400−k
第2の変換手段405−k
暗号サーバ410−1
第2の変換手段415−1
暗号サーバ410−k
第2の変換手段415−k
暗号サーバ440−1
第2の変換手段445−1
暗号サーバ440−k
第2の変換手段445−k
投票者端末100
表示装置101
入力装置102
機器側認証手段103
暗号データ作成手段104
投票者端末110
表示装置111
入力装置112
組織内基盤署名生成手段113
暗号データ作成手段114
投票者端末120
投票者端末130
投票者端末140
表示装置141
入力装置142
共通基盤署名生成手段143
暗号データ作成手段144
投票者端末150
認証サーバ300
投票サーバ200
有権者名簿データベース201
共通基盤署名検証手段202
第1の変換手段206
暗号化証明検証手段207
記録装置204
匿名復号システム500

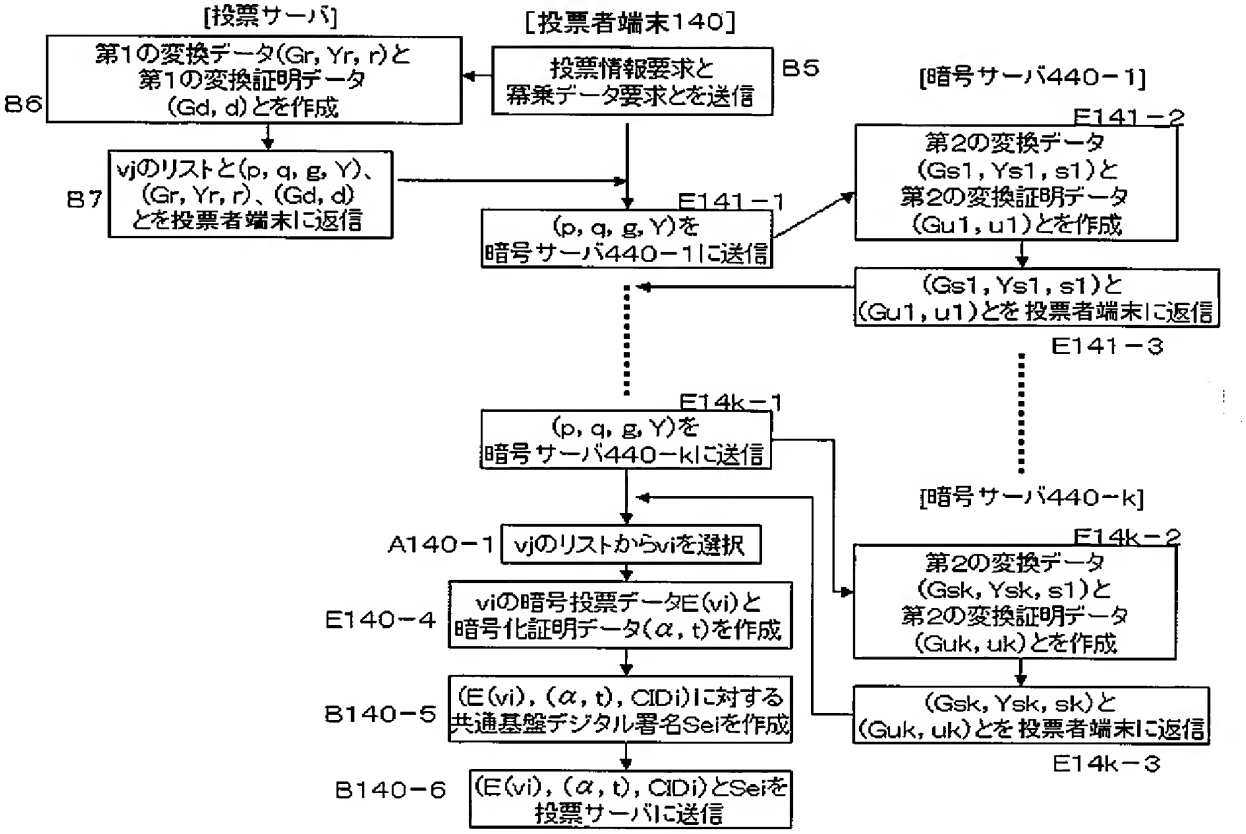
[図25]


[投票サーバ]
[投票者端末100]
第1の変換データ(Gr, Yr, r)と
第1の変換証明データ
(Gd, d)とを作成
B6
投票情報要求と
冪乗データ要求とを送信
B5
[暗号サーバ400−1]
E101−2
第2の変換データ
(Gs1, Ys1, s1)と
第2の変換証明データ
(Gu1, u1)とを作成
vjのリストと(p, q, g, Y)、
(Gr, Yr, r)、(Gd, d)
とを投票機器に返信
B7
E101−1
(p, q, g, Y)を
暗号サーバ400−1に送信
(Gs1, Ys1, s1)と
(Gu1, u1)とを投票者端末に返信
E101−3
E10k−1
(p, q, g, Y)を
暗号サーバ400−kに送信
[認証サーバ]
[暗号サーバ400−k]
A100−5
投票者の組織内識別子
IIDiの認証
A100−1
vjのリストからviを選択
E10k−2
第2の変換データ
(Gsk, Ysk, sk)と
第2の変換証明データ
(Guk, uk)とを作成
E100−4
viの暗号投票データE(vi)と
暗号化証明データ(α, t)を作成
A100−7
IIDiに対応する
共通識別子CIDiを取得
投票者の組織内識別子
IIDiの認証
(Gsk, Ysk, sk)と
(Guk, uk)とを投票者端末に返信
E10k−3
B100−8
(E(vi), (α, t), CIDi)に対する
認証サーバのデジタル署名
Sekを作成
A100−5
B100−9
(E(vi), (α, t)CIDi)とSekを
投票サーバへ送信
E(vi), (α, t)を
認証サーバに送信
B100−6

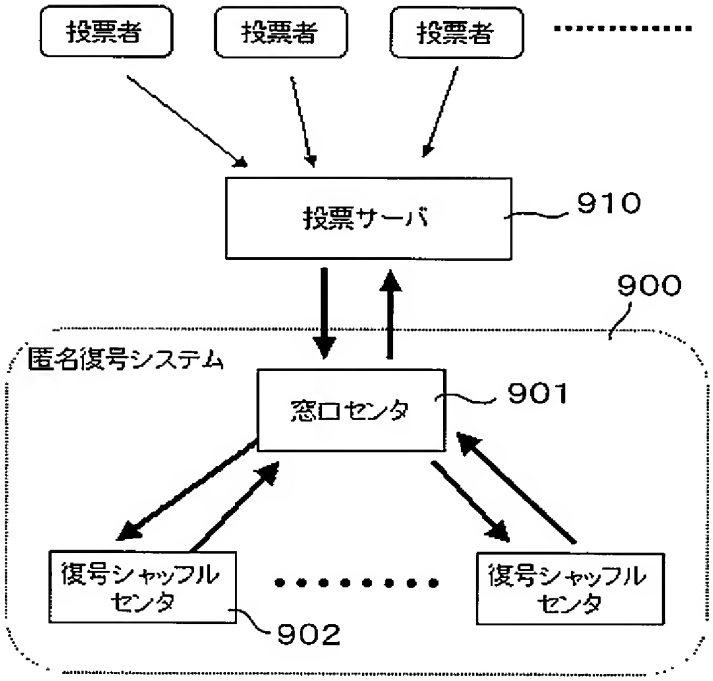
[図26]


[投票サーバ]
[投票者端末110]
第1の変換データ(Gr, Yr, r)と
第1の変換証明データ
(Gd, d)とを作成
B6
投票情報要求と
冪乗データ要求とを送信
B5
[暗号サーバ410−1]
E111−2
第2の変換データ
(Gs1, Ys1, s1)と
第2の変換証明データ
(Gu1, u1)とを作成
vjのリストと(p, q, g, Y)、
(Gr, Yr, r)、(Gd, d)
とを投票機器に返信
B7
E111−1
(p, q, g, Y)を
暗号サーバ410−1に送信
(Gs1, Ys1, s1)と
(Gu1, u1)とを 投票者端末に返信
E111−3
E11k−1
(p, q, g, Y)を
暗号サーバ410−kに送信
[認証サーバ]
[暗号サーバ410−k]
A110−1
vjのリストからviを選択
E11k−2
第2の変換データ
(Gsk, Ysk, sk)と
第2の変換証明データ
(Guk, uk)とを作成
E110−4
viの暗号投票データE(vi)と
暗号化証明データ(α, t)を作成
B110−7
Seiの正しさを検証
A110−8
IIDiに対応する
共通識別子CIDiを取得
B110−5
(E(vi), (α, t), IIDi)に対する
組織内向け
デジタル署名Seiを作成
(Gsk, Ysk, sk)と
(Guk, uk)とを 投票者端末に返信
E11k−3
B110−9
(E(vi), (α, t), CIDi)に対する
認証サーバのデジタル署名
Sekを作成
B110−10
(E(vi), (α, t), CIDi)とSekを
投票サーバへ送信
(E(vi), (α, t), IIDi)とSeiを
認証サーバに送信
B110−6

[図27]


[投票サーバ]
[投票者端末140]
第1の変換データ(Gr, Yr, r)と
第1の変換証明データ
(Gd, d)とを作成
B6
投票情報要求と
署名データ要求とを送信
B5
[暗号サーバ440−1]
E141−2
vjのリストと(p, q, g, Y)、
(Gr, Yr, r)、(Gd, d)
とを投票者端末に返信
B7
E141−1
(p, q, g, Y)を
暗号サーバ440−1に送信
第2の変換データ
(Gs1, Ys1, s1)と
第2の変換証明データ
(Gu1, u1)とを作成
(Gs1, Ys1, s1)と
(Gu1, u1)とを投票者端末に返信
E141−3
E14k−1
(p, q, g, Y)を
暗号サーバ440−kに送信
[暗号サーバ440−k]
A140−1
vjのリストからviを選択
E14k−2
第2の変換データ
(Gsk, Ysk, s1)と
第2の変換証明データ
(Guk, uk)とを作成
E140−4
viの暗号投票データE(vi)と
暗号化証明データ(α, t)を作成
B140−5
(E(vi), (α, t), CIDi)に対する
共通基盤デジタル署名Seiを作成
(Gsk, Ysk, sk)と
(Guk, uk)とを投票者端末に返信
E14k−3
B140−6
(E(vi), (α, t), CIDi)とSeiを
投票サーバに送信

[図28]


投票者
投票者
投票者
投票サーバ
910
900
匿名復号システム
窓口センタ
901
復号シャッフル
センタ
復号シャッフル
センタ
902

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/000532

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08, H04L9/32, G07C13/00, G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/08, H04L9/32, G07C13/00, G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Jitsuyo Shinan Toroku Koho	1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FLIE (JOIS), WPI, INSPEC(DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A Y	Kengo MORI, Kazue SAKO, Masaaki TAKIZAWA, Naoki SASAMURA, "Shuffle o Mochiita Denshi Tohyo System no Jiso", Heisei 14 Nen Denki Gakkai Denshi·Joho·System Bumon Taikai Koen Ronbunshu", 02 September, 2002 (02.09.02), Vol.2002, pages 421 to 424 (OS4-4)	1-6,12-16 7-11,17-20
Y	JP 2-151892 A (Matsushita Electric Industrial Co., Ltd.), 11 June, 1990 (11.06.90), Full text; all drawings (Family: none)	7-11,17-20

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 08 April, 2005 (08.04.05)	Date of mailing of the international search report 26 April, 2005 (26.04.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/000532

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Junji NAKAZATO, Hiroaki KIKUCHI, Shohachiro NAKANISHI, "Himitsu Counter Protocol o Mochiita Denshi Tohyo System no Keitai Joho Tanmatsu heno Jiso to Hyoka", Transactions of Information Processing Society of Japan, 15 August, 2003 (15.08.03), Vol.44, No.8, pages 1904 to 1912	1-20

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/000532

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-6, 12-16 relate to an anonymous electronic voting system or method for enabling electronic voting even in a voter terminal having no operation function for performing encryption processing.

The inventions of claims 7-11, 17-20 relate to an anonymous electronic voting system or method requiring a voter terminal to have an operation function for performing encryption processing.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／０００５３２

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／０８，Ｈ０４Ｌ９／３２，Ｇ０７Ｃ１３／００，Ｇ０６Ｆ１７／６０

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／０８，Ｈ０４Ｌ９／３２，Ｇ０７Ｃ１３／００，Ｇ０６Ｆ１７／６０

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国登録実用新案公報	１９９４－２００５年
日本国実用新案登録公報	１９９６－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

ＪＩＣＳＴファイル（ＪＯＩＳ），ＷＰＩ，ＩＮＳＰＥＣ（ＤＩＡＬＯＧ）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	森健吾，佐古和恵，瀧澤政明，笹村直樹，“シャッフルを用いた電子投票システムの実装”， 平成１４年電気学会電子・情報・システム部門大会講演論文集， ２００２．０９．０２，Vol.２００２， ｐ．４２１－４２４（ＯＳ４－４）	1-6, 12-16
Y		7-11, 17-20
Y	ＪＰ　２－１５１８９２　Ａ（松下電器産業株式会社） １９９０．０６．１１，全文，全図 （ファミリーなし）	7-11, 17-20

☒ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０８．０４．２００５	国際調査報告の発送日 26.4.2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 青木　重徳　　５Ｍ　４２２９ 電話番号　０３－３５８１－１１０１　内線　３５９７

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	中里純二，菊池浩明，中西祥八郎，“秘密カウンタプロトコルを用いた電子投票システムの携帯情報端末への実装と評価” 情報処理学会論文誌，２００３．０８．１５， Ｖｏｌ．４４，Ｎｏ．８，ｐ．１９０４－１９１２	１－２０

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／０００５３２

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－６，１２－１６に係る発明は、電子投票を暗号処理を行う演算機能を有しない投票者端末でも行えるようにした匿名電子投票システムないし方法に関するものである。

請求の範囲７－１１，１７－２０に係る発明は、投票者端末に暗号処理を行う演算機能を備えることを必須とする匿名電子投票システムないし方法に関するものである。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。